UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de la auditoria de sistemas en el servicio de atención al usuario en el Ministerio de Educación

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

AUTOR:

Segura Gutarra, Stewart (ORCID: 0000-0001-7425-8539)

ASESOR:

Hilario Falcón, Francisco Manuel (ORCID: 0000-0003-3153-9343)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LIMA – PERÚ

2018

Dedicatoria

Dedico el presente trabajo:

A mi esposa en Dios, mi madre que fue mi inspiración de esfuerzo, dedicación y aspiraciones, mis amados hijos que sacrificaron tiempo en familia para poder alcanzar mis metas.

Agradecimiento

A los docentes y a la Universidad César Vallejo por mi formación académica y mi asesor Manuel Hilario por su valioso apoyo.

PRESENTACIÓN

Señores miembros del jurado:

En cumplimiento de las normas establecidas en el Reglamento de Grados y Títulos de la Universidad César Vallejo presento ante ustedes la tesis titulada "Implementación de la auditoria de sistemas en el servicio de atención al usuario en el Ministerio de Educación" la misma que someto a vuestra consideración y espero que cumpla con todos los requisitos de aprobación para obtener el título profesional de Ingeniero de Sistemas.

La presente investigación consta de seis capítulos; el primer capítulo, se enfoca en la introducción de la tesis en la cual se expone la problemática del trabajo de investigación, teorías relacionadas, trabajos previos y el sustento de la tesis; asimismo se presentan las justificaciones y objetivos, para este punto se precisa el objetivo general: Determinar el efecto de la auditoría de sistemas para el servicio de atención al usuario en el Ministerio de Educación y los tres objetivos específicos, el primero: Determinar el efecto de la Implementación de la auditoría de sistemas para el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación, el segundo: Determinar el efecto de la Implementación de la auditoría de sistemas para el diagnóstico de incidentes en el servicio de atención al usuario en el Ministerio de Educación, el tercero: Determinar el efecto de la Implementación de la auditoria de sistemas para la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación. Asimismo, la hipótesis general y las específicas que se plantearon en la investigación. El segundo capítulo, puntualiza la metodología explicando el tipo de diseño e investigación que se aplicará, se determina la población, muestra en la cual se validará la auditoria para el registro, diagnóstico y resolución de incidentes, donde también se desarrollan los datos, instrumentos y técnicas para recolectar los datos. El tercer capítulo, muestra los resultados obtenidos de cada indicador propuesto al realizar las pruebas antes y después de implementar la auditoría, con algunas tablas como gráficos para realizar una interpretación más comprensible para el leyente. El siguiente capítulo, contiene la validación de los resultados obtenidos de varias investigaciones con el propósito de defender o diferir de ellos, en el caso de no coincidir con sus resultados. El siguiente capítulo, describe las conclusiones del trabajo de investigación de cado uno de los indicadores, tomando de referencia nuestros resultados. Para terminar en el capítulo seis, se plantea las recomendaciones para futuros trabajos de investigación.

Se espera señores miembros del jurado que la presente investigación se ajuste a los requerimientos establecidos y que este trabajo de origen a posteriores estudios.

Stewart Segura Gutarra

Índice

Índice de Tablas

Índice de Figuras

RESUMEN

La presente investigación plantea como objetivo la implementación de una auditoría de sistemas en el servicio de atención al usuario en el Ministerio de Educación logrando reducir incidentes en el registro, diagnóstico y tiempos de resolución, la metodología MAGERIT nos permite elaborar una matriz de riesgos y el modelo COBIT 5.0 nos brinda los lineamientos para realizar una auditoría interna, la cual tiene como conclusión que se tuvo una reducción considerable en el porcentaje de incidentes, por esta razón se propone se realice la auditoría de sistemas para el servicio de atención al usuario. Para finalizar, en cada proyecto se requiere obtener una mejora continua; por ello, se recomienda a futuros investigadores que les pueda parecer interesante esta tesis puedan o traten de incorporar nuevas ideas a la auditoría.

Palabras clave: auditoría, registro, diagnóstico, resolución, mejora de servicio, atención al usuario.

ABSTRACT

The present investigation raises as objective the implementation of a systems audit for the user service in the Ministry of Education managing to reduce incidents in the registry, diagnosis and resolution times, the MAGERIT methodology allows us to elaborate a matrix of risks and the COBIT 5.0 model provides the guidelines for an internal audit, which concludes that there was a considerable reduction in the percentage of incidents, for this reason it is proposed to implement the systems audit aimed at improving the service of attention to the user. Finally, each project requires continuous improvement; therefore, it is recommended to future researchers that this thesis may be interesting to them or they may try to incorporate new ideas to the implementation of the audit.

Keywords: audit, registry, diagnosis, resolution, service improvement, user service.

I. INTRODUCCIÓN

1.1 Realidad problemática

Con fecha 30 de octubre de 2006, es aprobado en el Estado Peruano la normatividad que regula el control interno, dicho documento se oficializó en el diario oficial "El Peruano", mediante una resolución interna en la Contraloría de la República (RC N° 320-2006-CG), la cual tiene un ámbito de aplicación en todos los órganos que componen el Estado. Asimismo, se dispone a todos los órganos de línea y apoyo de esta, en el marco de las competencias funcionales que le fueron asignadas, elaboren y propongan lineamientos (directivas) que, a modo de complemento, estimen convenientemente necesarias para la óptima regulación, en relación con todo lo vinculado al control interno de sus ámbitos de actuar. Dictaminando además que, la máxima autoridad de la Gerencia Central de Desarrollo y la Escuela Nacional de Control sean las responsables de las actividades de sensibilización, capacitación y difusión necesarias de las normas de control interno. En aplicación de lo dispuesto, se desarrollaron diferentes metodologías para el cumplimiento y control de la norma, entre estas, la más aplicada para auditoría en el sector público es el modelo COBIT 5.0, la cual establece los objetivos para la gestión de peticiones e incidentes de servicio, cuyos objetivos son: asegurar la disponibilidad de los servicios que serán utilizados, incidentes resueltos de acuerdo con los niveles de servicio acordados, la resolución de peticiones.

Para ISACA:

Usar COBIT® 5 principalmente como un recurso educativo para la gobernanza de TI empresarial (GEIT), aseguramiento, riesgos y profesionales de la seguridad no afirma que el uso de cualquiera de los Trabajos garantizará un resultado exitoso. El Trabajo no debe considerarse como inclusivo de toda la información, procedimientos y pruebas adecuadas o excluyentes de otra información, procedimiento y pruebas que estén razonablemente dirigido a obtener los mismos resultados. Al determinar la corrección de cualquier información, pruebas específicas o procedimiento, los lectores deben aplicar su propio criterio profesional a las circunstancias específicas que presentan los sistemas particulares o el entorno de tecnología de la información (2012, p 2).

El órgano rector normativo en Educación (Minedu) con fecha de fundación en el año 1837, a la fecha tiene más de 200 servidores públicos contratados, bajo diferentes modalidades de contrato, en la OTIC (Oficina de Tecnologías de TIC), a su vez esta oficina cuenta con unidades de trabajo que cumplen con funciones que necesitan el uso de marcos de buenas prácticas en gestión de servicios, bajo el enfoque de ITIL, una de estas unidades denominada USAU (Unidad de Servicios), centrará nuestro proyecto de investigación. Esta unidad orgánica cuenta con funciones definidas mediante Decreto Supremo N° 001-2015-MINEDU, las cuales son:

- "Diseñar e implementar los procesos, procedimientos y métricas que permitan ofrecer en forma eficiente y oportuna la atención y ayuda técnica a los usuarios de los servicios informáticos del Ministerio".

- “Brindar el soporte técnico a los sistemas operativos, software de base, aplicaciones y comunicación a los órganos y unidades orgánicas del Ministerio”.
- “Supervisar el mantenimiento preventivo y correctivo de los equipos informáticos asignados al personal del Ministerio”.
- “Orientar y capacitar al personal del Ministerio sobre el uso de las herramientas y recursos informáticos”.
- “Supervisar el cumplimiento de las normas y procedimientos dictados para el adecuado uso de los equipos y servicios informáticos en red”
- “Otros que en el marco de sus competencias le sean asignadas por la Oficina de Tecnologías de la Información y Comunicación”.

En relación con la penúltima función, el jefe (e) de la USAU manifiesta su preocupación por asegurar el cumplimiento del proceso y procedimientos de incidentes (graves y de seguridad de la información), las cuales no cuentan con indicadores definidos; asimismo, manifiesta la necesidad de implementar controles que aseguren dicho cumplimiento. Se asume que esta falencia origina un impacto significativo en la OTIC, debido a las dificultades que se suscitan para la toma de decisiones y poder mitigar el riesgo de la percepción negativa de la imagen institucional y/o problemas legales que pudieran presentarse. Por otro lado, los colaboradores de la USAU desconocen la probabilidad del impacto ante la falta de ejecución del procedimiento de incidentes graves y de seguridad en los servicios de TI del Minedu. De persistir con esta realidad, los responsables de la USAU podrían incurrir en faltas administrativas procedimentales y sufrir procesos administrativos o legales. Por estas razones, se decidió elaborar un proyecto de investigación en la USAU e implementar una auditoría de sistemas utilizando COBIT 5.0 y la auditoría interna empleando MAGERIT como metodología para el análisis de los riesgos en la gestión, con el fin de asegurar la disponibilidad para que los servicios sean utilizados, contar con la atención de incidencias y que estas sean resueltas según los SLA del servicio, así como la atención oportuna de peticiones; obteniendo finalmente, la satisfacción del usuario y la mejora de la imagen de la OTIC en el Minedu.

1.2 Trabajos previos

Para tener información sobre situaciones similares, se consultaron diversos estudios.

Agramonte (2016) indicó:

Como objetivo principal de este trabajo de investigación se realizó una Auditoría del Sistema de Seguridad de Información del Hospital III José Cayetano Heredia – Castilla, el cual permitió mejorar la gestión de la información, de acuerdo con las características, la investigación fue enfocado cuantitativo; asimismo, el tipo de investigación fue descriptivo no experimental y de corte transversal, utilizando la técnica de encuesta y se aplicó como instrumento un cuestionario. (Agramonte, 2016)

Los resultados obtenidos demostraron que el 38% de los trabajadores encuestados expresaron que la actual seguridad lógica se encontraba en un nivel 1 – Inicial; el 69% de los trabajadores encuestados indicaron que la seguridad de las aplicaciones están en un nivel 3 – definido y por último el 55% de los trabajadores encuestados refirieron también en el nivel 3 – definido para la actual administración del centro de procesamiento de datos. (Agramonte, 2016)

Se concluyó que el nivel de seguridad del Sistema de Información del Hospital III José Cayetano Heredia – Castilla, se encuentra en el nivel 2 – Repetible, según los niveles de madurez del modelo de referencias de COBOT 4.1. (Agramonte, 2016)

Gago (2013) indicó:

El objetivo principal de esta investigación es determinar si la implementación del área de auditoría interna afectará los resultados de la gestión financiera de las cooperativas de servicios múltiples en Lima Metropolitana; debido al análisis de las teorías existentes e información teórica sobre este tema, y el uso de Una herramienta (encuesta) para obtener información directa sobre las personas involucradas en el tema, por lo que el trabajo es descriptivo y aplicado. (Gago, 2013)

Los resultados obtenidos demostraron que el 95% de los encuestado está de acuerdo con la implementación de una oficina de auditoría interna como una alternativa para evaluar el accionar de las cooperativas de servicios múltiples de Lima Metropolitana; Asimismo, el 85% de encuestados están de acuerdo que es importante realizar una evaluación de estado (auditoría interna) de las operaciones del negocio; el 95% de encuestados están muy de acuerdo con los productos de la eficiente administración de los recursos en las cooperativas y finalmente el 100% de encuestados está de acuerdo que la toma de decisiones oportuna es trascendental para el logro de objetivos en estas cooperativas. (Gago, 2013)

La conclusión es que la auditoría interna, a través de su tecnología, procedimientos y todos sus mecanismos, afecta la gestión de la Cooperativa de Servicios Metropolitana de Lima y le permite detectar errores y tomar medidas correctivas o preventivas para mejorar el statu quo de estas organizaciones. (Gago, 2013)

Huamán (2014) indicó:

El objetivo primordial de este proyecto de investigación buscó realizar un documento procedimental de auditoría de cumplimiento y enmarcada en estándares internacionales de seguridad de la información. Las cuales son aplicadas al sector privado y público, utilizándose a su vez en marcos de trabajo gubernamentales como COBIT 5.0, que

puede ser utilizado para procesos de implementación del estándar internacional de seguridad de la información más reciente "NTP-ISO/IEC 27001:2008" teniendo como único fin la mejora de la gestión de la seguridad de la información. (Huamán, 2014)

Los resultados que se obtuvieron demostraron que existe un cumplimiento significativo de la empresa (del estado peruano), el cual alcanzo un valor porcentual de 91.66% del dominio cinco (5) y un valor porcentual de 83.33% correspondiente al dominio siete (7) del estándar internacional de seguridad de la información anterior (2007) como parte de un componente de implementación del estándar de seguridad vigente (2008). (Huamán, 2014)

Se concluye identificando que las validaciones realizadas fueron efectivas y que el proyecto hecho, complementó de manera idónea la finalización de los estudios profesionales correspondientes, identificando además que lo proporcionado, como herramienta, puede ser utilizada para el proceso de evaluación, asegurando el cumplimiento normativo ("NTP-ISO/IEC 17799" y "NTP-ISO/IEC 27001"), la cual debe realizarse en las organizaciones públicas del Perú que deban cumplir este ámbito de aplicación (régimen) y que están obligadas a implementar. (Huamán, 2014)

Rafael y Castillo (2016) indicaron:

Como objetivo principal de este trabajo de investigación se buscó describir, especificar, aplicar normas y emitir recomendaciones que ayuden en la mejora de las atenciones informáticas (tecnologías de la información) en la unidad de servicios e informática del "Hospital Las Mercedes de Chiclayo", con el fin de incrementar la efectividad en el área indicada; para la investigación se usó la metodología PDCA, la cual permite eliminar procesos repetitivos, permitiendo reducir los tiempos y mejorar el análisis de cada proceso. (Rafael y Castillo, 2016)

Los resultados obtenidos demostraron que, según los objetivos de control detallados en COBIT 5.0, se encontraron que nueve (9) de los 19 objetivos de control evaluados, son efectivos; por lo que, el resultado es favorable con excepciones, las cuales se deben a la no contratación de recurso humano en el área; asimismo, no existe un proceso que permita asegurar la mantención del conocimiento (know how) y los niveles de competitividad de las personas a cargo de TI. Además, se identificó que no se tienen definidos las estructuras clasificatorias de las fallas o errores (incidentes) y las solicitudes de servicio, las cuales permiten que exista una priorización de atención, de manera que se realice una eficaz y eficiente resolución. También, una de estas excepciones se manifiesta por una falta de análisis e información del rendimiento del área de CSI, la cual debe notificar de manera periódica a la Gerencia. Por otro lado, no se planifican ni estudian las iniciativas planteadas de aseguramiento que permitirían

diagnosticar los riesgos asociados e identificar los procesos críticos de los servicios de TI. (Rafael y Castillo, 2016)

Se concluye que, al aplicar la metodología PDCA se pudo realizar el desarrollo del informe final de auditoría, el cual plantea observaciones que identificaron que en cada una de estas se encontraron riesgos que se pueden generar al no ser levantadas las observaciones; asimismo, se emitieron recomendaciones para subsanar las observaciones hechas en la auditoría aplicada. En conclusión, la auditoría realizada es favorable con excepciones. (Rafael y Castillo, 2016)

Aroca (2016) indicó:

Como objetivo primordial de este trabajo de investigación se buscó identificar el impacto generado por la realización de una auditoría interna en la gestión de la empresa de transportes Guzmán S.A, la cual está ubicada en la ciudad de Trujillo, la investigación fue realizada el año 2015; para este trabajo se utilizaron métodos analíticos, inductivos, deductivos, sintéticos y aplicando técnicas como la observación directa, analítica, documental, encuesta y entrevistas. (Aroca, 2016)

Los resultados obtenidos demostraron que, la empresa de transportes auditada se concentrará y tendrá mayor detalle de atención en la mejora de su gestión administrativa, así como a la superación de los puntos críticos identificados. La auditoría interna permitirá lograr un mayor beneficio económico y un eficaz cumplimiento de la misión de la organización; es decir, le permitirá conseguir los resultados esperados. (Aroca, 2016)

Se concluye que, la auditoría realizada en la empresa de transportes (Transportes Guzmán S.A) fue exitosa, teniendo en consideración que el trabajo realizado por el auditor interno, en relación a los controles aplicados, fue oportuno y profesional, ofreciendo confianza a la Alta Dirección y el conjunto de accionistas relacionados a los cumplimientos regulatorios y buenas prácticas en gestión del negocio de dicha organización; por lo tanto, el trabajo realizado incurre positivamente a esta empresa de transportes, ubicada en la ciudad de Trujillo. (Aroca, 2016)

Huamán (2018), indicó:

El objetivo primordial de este proyecto de investigación buscó diseñar un control interno (auditoría) para obtener mejora en los procesos financieros en la empresa de Representaciones y Distribuciones del Norte "REYDINOR S.A.C", la cual a través de análisis de técnica contable determinó y evidenció las deficiencias en el manejo de la gestión financiera. (Huamán, 2018)

Los resultados obtenidos demostraron que el 100% de los trabajadores de la empresa manifestaron que no se cuenta con un inventario de activos actualizado, no se cuenta con recursos de TI adecuados para el cumplimiento de sus funciones, no se cuenta con reportes para la validación de recibos de cobranzas de clientes y no se realizan auditorías externas. (Huamán, 2018)

Se concluyó que existen dificultades en el control del personal que labora en dicha empresa, las funciones de los empleados se encuentran establecidas y se manejan mediante un reglamento interno; en síntesis, la empresa REYDINOR SAC podría afectarse, ya que casi todos sus clientes tienen retrasos en los pagos de sus pedidos. (Huamán, 2018)

Mariñas (2015), indicó:

Como objetivo principal de este trabajo de investigación se buscó desarrollar una auditoría informática a la red de datos del Hospital Tingo María, con el fin de diagnosticar el estado actual de la organización, proponiendo mejoras que aseguren el eficiente funcionamiento de la red corporativa. (Mariñas, 2015)

Los resultados obtenidos demostraron que no se cuenta con software antivirus en la institución, tampoco existe un firewall que controle el tráfico y los servicios de la red corporativa, infraestructura de comunicaciones con presencia de humedad, hongos y deterioro del recinto y la falta de conexión de la sala de equipos con el sistema de pozo a tierra en dicha entidad. (Pingo, 2015)

Se concluyó que la auditoría informática permitió identificar las vulnerabilidades de la infraestructura tecnológica del Hospital Tingo María, ayudando a su vez, en base a la Norma Técnica Peruana NTP-ISO/IEC 27001, realizar las recomendaciones de control para mejorar su infraestructura. (Mariñas, 2015)

Gonza (2017), indicó:

El objetivo primordial de este proyecto de investigación buscó realizar el plan estratégico de auditoría e identificar el comportamiento en seguridad y salud ocupacional en la empresa especializada CONSEM E.I.R.L de Pataz, para la evaluación de esta investigación se utilizó como referencia los estándares y criterios de las normas OHSAS 1001:2007. (Gonza, 2017)

Los resultados obtenidos demostraron que la auditoría es eficiente y permitió a la entidad la autorización de la alta dirección para que estas prácticas se realicen periódicamente, como mínimos dos (02) veces por año. (Gonza, 2017)

Se concluyó que, toda empresa privada que quiera ser competitiva y quiera perdurar en el mercado debe realizar revisiones periódicas y mejorar constantemente su sistema de gestión de riesgos laborales. (Gonza, 2017)

Gavilán y Meléndez (2016), indicó:

Como objetivo principal de este trabajo de investigación se buscó mostrar e identificar los incidentes que afectan directamente a la calidad de su gestión en la organización denominada: "Grupo Silvestre S.A.C"; utilizando para dicho fin el uso de la metodología descriptiva/correccional para establecer la descripción y relación entre variables. (Gavilán y Meléndez, 2016)

Los resultados obtenidos demostraron que este proyecto y la gestión de calidad desarrollada fue exitosa, la cual tuvo fundamentación de diferentes autores, permitiendo ayudar a la comprobación de los resultados obtenidos, confirmando la suposición (hipótesis) proyectada, señalando que la auditoría realizada favorece directamente a la gestión de la calidad de esta organización. (Gavilán y Meléndez, 2016)

Se concluyó que, ante la falta de la documentación procedimental de auditorías en la organización auditada, se generan problemas de eficiencia en los resultados obtenidos de la gestión de riesgo y dirección en los equipos de trabajo de logística, producción, almacén, ventas y productos terminados. (Gavilán y Meléndez, 2016)

Estrella (2017), indicó:

Como objetivo principal de este trabajo de investigación se buscó determinar la auditoría operativa evaluando la eficiencia de la gestión administrativa de la Universidad Privada de Tacna en los periodos 2014, 2015 y 2016; para dicho fin fueron empleadas las evaluaciones a través de análisis financieros. (Estrella, 2017)

Los resultados obtenidos demostraron que se puede afirmar que el indicador óptimo es la rentabilidad, siendo que los periodos 2015 – 2016 se obtuvieron avances favorables para la institución en comparación con el periodo anterior. (Estrella, 2017))

Se concluyó que los acontecimientos en esta investigación de auditoría operativa, se pudo comprobar el análisis financiero que la gestión de la Entidad realizó en los periodos evaluados (2014 – 2015 y 2016), evidenciando que es favorable en los resultados obtenidos para la institución a través de los años. (Estrella, 2017))

Chávez (2017), indicó:

El objetivo primordial de este proyecto de investigación buscó mejorar los procesos y procedimientos realizados en el "Banco Financiero" – Sede Chimbote y con mayor enfoque en el equipo de crédito, aplicando la auditoría informática, en la investigación se utilizó el estándar COBIT como modelo que permitió auditar la gestión y control de los sistemas de información y tecnología en la Entidad. (Chávez, 2017)

Las deducciones obtenidas demostraron que, se logró verificar el incremento considerable de satisfacción de clientes en la Entidad financiera ubicada en la Sede Chimbote; así también, permitió generar un plan de acción con posible mejoras en los procesos y procedimientos del equipo de crédito, que a su vez, permitirán garantizar a la Entidad los pilares de la seguridad de la información (integridad, confidencialidad y confiabilidad); además, se pudo viabilizar la solvencia económica de esta investigación. (Chávez, 2017)

Se concluyó que se pudo elaborar un plan de acción con las posibles mejoras en los procesos y procedimientos del equipo de crédito, las cuales fueron consideradas en la aplicación de la auditoría informática, las recomendaciones realizadas contribuirán con la mejora de falencias halladas en la Entidad financiera. (Chávez, 2017)

Wither (2014) indicó:

Como objetivo principal de este trabajo de investigación se buscó proponer una Auditoría Interna de Sistemas, el cual será aplicado a una Aerolínea doméstica ecuatoriana; para ello, se tomó como marco de trabajo COBIT 5, el cual facilitó el análisis de gobierno y gestión de TI, provisionando una metodología y un marco para analizar los riesgos en TI. (Wither, 2014)

Los resultados obtenidos demostraron que es necesaria la formalización de la Auditoría Interna de Sistemas; asimismo, según el análisis de riesgos se pudo determinar que es necesario un Plan de actividades más extenso. (Wither, 2014)

Se concluyó que se debe considerar las necesidades o inquietudes de usuarios claves y estar alineados con los riesgos y expectativas del rol de Auditoría Interna de Sistemas, que se puedan tener. (Wither, 2014)

Eraso y Guerrero (2015) indicaron:

El objetivo básico del proyecto de investigación es revisar la seguridad de la información de la empresa Expreso Juanambú (empresa dedicada a los servicios de transporte urbano de pasajeros) con el fin de utilizar estándares internacionales de auditoría para verificar las operaciones de la empresa y el marco metodológico MAGERIT para análisis de riesgos. (Eraso y Guerrero, 2015)

Las inferencias extraídas muestran que el personal de la empresa ha sido capacitado para el desempeño responsable de sus funciones, la estructura jerárquica de la empresa cuenta con un sistema de gestión bien organizado, y la dirección de la empresa es responsable de la toma de decisiones, y se constata que las autoridades competentes de más alto nivel tienen una actitud positiva hacia el desarrollo de las actividades de manera relevante. , El entorno de trabajo es una de las cooperaciones altamente profesionales entre todos los empleados. (Wither, 2014)

Se concluyó que, al implementar COBIT y la normativa ISO-27000 en la empresa de transporte urbano de pasajeros, mejorará los estándares de calidad, fiabilidad y gestión de los servicios de TI; asimismo, reducirán los riesgos, incidentes y fallas en la ejecución de sus procesos. (Wither, 2014)

Lara (2015), indicó:

Como objetivo principal de este trabajo de investigación se buscó obtener resultados propicios que permitan determinar los pasos correspondientes para realizar este proyecto; en esta investigación se utilizó como marco metodológico la norma ISO 27001 en la empresa MAINT de la ciudad de Guayaquil. (Lara, 2015)

Los resultados obtenidos demostraron que existe un porcentaje menor de trabajadores que tienen claro los lineamientos de seguridad de la información, en relación con el control de accesos, el 18% del personal respalda su información a diario como política de seguridad, el 24% no tiene como disciplina un mantenimiento periódico de sus equipos de cómputo; además hay diversas. (Lara, 2015)

Se concluyó que, contar con una estructura formal con lineamientos definidos de seguridad informática y aplicando la norma ISO 2001, se garantizará el desarrollo de los procesos en la Entidad y la optimización de estos. (Lara, 2015)

Rivera y Zambrano (2015), indicó:

Como objetivo principal de este trabajo de investigación se buscó la evaluación de los niveles de cumplimiento de las aplicaciones de buenas prácticas, algunos estándares y algunas normas de control interno de TI en el órgano de control del gobierno ecuatoriano (Contraloría General del Estado Ecuatoriano), en relación a procesos, lineamientos (políticas) y procedimientos de los recursos tecnológicos existentes en la Entidad; para ello, se aplicó la metodología de la Norma ISO 27000 y se determinaron los hechos de mayor relevancia. (Rivera y Zambrano, 2015)

Los resultados obtenidos demostraron que se evidenciaron los principales hallazgos ocasionados en la Entidad determinaron que la unidad orgánica auditada cuenta con políticas genéricos de control para el mantenimiento de la infraestructura tecnológica; sin embargo, no aplica de manera correcta las normas mencionadas con anterioridad, evidenciándose el alto riesgo y su baja confianza de sus procesos. (Pingo, 2015)

Se concluyó que resulta conveniente la ejecución de las normas que permitan dominar más en la organización y responsabilidad, minimizando significativamente los riesgos en la infraestructura tecnológica de la Entidad. (Pingo, 2015)

1.3 Teorías Relacionadas al Tema

1.3.1 Auditoría interna:

Santillana (2013), indicó que:

Los procesos de evalaución interna son una profesión cuyas actividades involucran a la contribución con las Entidades, con su gobernanza colaborativa y con una administración enfocada con el logro de los objetivos, y para ello se apoyará recurrentemente en una metodología sistemática que permita analizar el procesos de negocio, así como actividades y los documentos procedimentales relacionados con los grandes desafíos de la organización. Todo esto conlleva en la recomendación de alternativas de solcuión. Es una fucnión practicada por personas dedicadas a la auditoría interna con un extraordinario conocimiento del negocio corporativo, sistematización y documetos procedimentales que tienen como objetivo brindar seguridad mediante regulaciones interiorizadas e instauradas y que serán convenientes para la mitigación de los riesgos, con miras al cumpleimiento de las metas trazadas y loss objetivos estimados por la empresa, mediante la entrega de un diagnóstico interno al despacho gerencial y adminsitrativo, respuestas que puedan

percibirse (cualitativas), otros cuantitavios, otros con independencia, en las que se puedan confiar, oportunos y ecuanimes. (Santillana 2013, p.14)

Asimismo, Muñoz también nos indicó lo siguiente:

De lo antes descrito, señalamos que los ámbitos de aplicación para los diagnósticos internos (auditorías) evolucionaron en demasía, contemplando desde su uso, en relación con los aspectos contables, hasta su utilización en unidades orgánicas y disciplinas de que son componentes especiales (ingeniería, medicina y sistemas de cómputo).

Obviamente, juntamente con este avance, tenemos registrado el desarrollo de técnicas, normativas metodológicas, procedimentales y herramientas de cada una de estas (tipos de auditorías), así también una visión característica y especializada en la utilización de técnicas de común uso por las unidades orgánicas que serán evaluadas.

En razón a los cambios constantes, indicaremos cual es el concepto más extenso del diagnóstico interno (auditoría), para posteriormente ser analizado por la RAE (Real Academia Española) y posteriormente, ya con la conceptualización clara, remitir una propuesta que clasifique los tipos de auditoría.

De manera general, podemos indicar que la definición propuesta para el diagnóstico interno (auditoría) es la que sigue: “Es la revisión independizada de algunas tareas o actividades, que cuenta con funciones puntuales, con resultantes o sistematizaciones de una organización administrativa, la cual fue realizada por una persona preparada (profesional) y capacitada en auditorías, con el objetivo de realizar una evaluación de su ejecución, y en razón a dicho análisis, podremos emitir las opiniones de autorización relacionada a la razón de sus resultantes y los cumplimientos de ejecución. (Muñoz 2013, p.10)

1.3.2 Clasificación de los tipos de auditorías

Según Muñoz, se clasifica a la auditoría de la siguiente manera:

Dando inicio al estudio realizado, proponemos que la analítica de las conceptualizaciones anteriores se hagan bajo el amparo de la clasificación siguiente de las tipificaciones de los diagnóticos internos (auditorías), esto con la finalidad de identificar las características, criterios y especificaciones de esta profesión. Luego nos enfocaremos puntualmente en las conceptualizaciones y las mejores definiciones de las auditorías de sistema computacional. (Muñoz 2013, p.13)

La descripción clasificatoria propuesta está considerada en el siguiente cuadro:

Las auditorías por su lugar de aplicación:

- Una auditoría externa.
- Una auditoría interna.

Las auditorías por su área de aplicación:

- Las auditorías financieras.
- Las auditorías admisnitrativas.
- Las auditorías operacionales.
- Las auditorías integrales.
- Las auditorías gubernamentales.
- Las auditorías de sistemas.

Las auditorías especializadas en áreas específicas:

- Las auditorías en las áreas médicas.
- Las auditorías dedicadas al desarrollo de obras y construcciones.
- Las auditorías fiscales.
- Las auditorías laborales.
- Las auditorías para proyectos de inversión.
- Las auditorías de las cajas chicas o cajas mayores.
- Las auditorías de los manejos de mercancías.
- Las auditorías ambientales.
- Las auditorías de sistemas.

Las auditorías de sistemas computacionales:

- Las auditorías informáticas.
- Las auditorías con las computadoras.
- Las auditorías sin computadoras.
- Las auditorías de la gestión informática.
- Las auditorías de los sistemas de cómputo.
- Las auditorías alrededor de las computadoras.
- Las auditorías de la seguridad de los sistemas computacionales.
- Las auditorías a los sistemas de redes.
- Las auditorías integrales a los centros de cómputo.
- Las auditorías de la ISO-9001 a los sistemas computacionales.
- Las auditorías ergónomicas de sistemas computacionales.

1.3.3 Las auditorías internas

Según Muñoz, indicó que las auditorías internas son:

Dentro de lo realizado para las tipologías de la evaluación, el profesional que realiza la auditoría es un trabajador interno y dependiente de la oraganización a tratar; por lo tanto, esta persona está involucrado dentro de su operación regular; con este

detalle, el profesional a cargo del diagnóstico podrá tener dependencia directa de las autoridades de su empresa, pudiendo esta condición influir en su juicio al remitir la evaluación de las unidades que componen su organización. La conceptualización sugerida es:

Son las validaciones que realiza un profesional que realiza un diagnóstico o evaluación (auditorías), el mismo que tendrá una relación laboral directa o subordinada con la organización donde se realizará la auditoría, con el objetivo de realizar la evaluación de forma interna en relación al cumplimiento y desempeño de las activiadades, funciones y operaciones que se realizan en la organización y sus equipos adminsitrativos, asimismo diagnosticaremos la razonabilidad en el envío de las resultantes financieras. El principal objetivo requerido es tener un dictamen interno enrelación de las actividades realizadas en la organización, la cual nos permite tener el diagnóstico del actuar adminsitrativo, funcional y operativo de los trabajadores y funcionarios de las unidades orgánicas que son auditadas. (Muñoz 2013, p.15)

Ventajas:

Teniendo en cuenta que el profesional que realiza la auditoría es de la misma organización, este conoce exactamente las operaciones, actividades y unidades orgánicas; por ello, su evaluación tendrá mayor profundidad y conocimiento de las funciones, actividades y problemáticas de la organización. En tal sentido, el informe que realice tendrá mayor valor.

Los informes realizados por los auditores internos, muy independientes de sus resultantes, sólo se utilizan de manera interna, es decir que no salen de la organización, ya que estas será utilizadas por las máximas autoridades de la organización auditada.

El diagnóstico realizado se abastecerá sólo de recursos propios de la organización, por ello, es insignificante una reproducción adicional para la organización auditada.

Resulta de gran utilidad para el encaminamiento ideneo de la organización, ya que nos permitirá identificar problemáticas y desviaciones en tiempo real.

Es posible realizar programas concretos de diagnóstico o evalaución como un apoyo a las autoridades de la organización, la cual permitirá a los altos funcionarios en las evaluaciones y toma de decisiones de negocio.

Desventajas:

Su autentidad, el alcance y su confiabilidad estan límitadas, esto se debe a la injerencia que tienen los altos funcionarios de la organización sobre el procedimiento para la evaluación y posterior emisión del informe.

En ciertas oportunidades la opinión del profesional a cargo de la auditoría no es absoluta, ya que al trabajar en la misma organización donde se realiza esta auditoría, se presentarán presiones, intereses y compromisos al realizar su evaluación.

Es posible que se presenten con mucha frecuencia vicios laborales del prosional a cargo de la auditoría, podría presentarse en forma de la utilización de las técnicas y herramientas en la aplicación de la auditoría, como en la forma de evalaución y emisión del informe de la auditoría.

1.3.4 Las auditorías informáticas

Asimismo Muñoz, indicó que la clasificación de las auditorías informáticas está identificada como:

Motivación de la especialidad en las actividades computacionales, asimismo por lo espectacular de los avances que tuvieron estos sistemas en los últimos años, tenemos hoy en día nuevas necesidades de evaluación para los profesionales a cardo de las auditorías, los mismos que necesitan especializarse cada vez más en los sistemas para que puedan enfocarse a estas auditorías. Ante ello, nace la necesidad de evaluación no sólo para los sistemas, sino además la data (información), cada uno de sus componentes y todo lo que se relacione con esos sistemas. Definiremos entonces la siguiente propuesta:

Se le denomina a la evaluación técnica que tiene especialización y es minuciosa y que son realizadas a los sistemas, software e información y computacionales usados por la organización, ya sean estos individuales, de redes, compartidas, sus mobiliarios, instalaciones, telecomunicaciones, equipos periféricos y otros componentes.

La revisión es realizada de manera similar a la gestión de TI, aprovechando sus recursos, todas las medidas de seguridad y los bienes necesarios que son de consumo para la operatividad del centro de cómputo. El objetivo primordial y fundamental es realizar la evaluación del uso conveniente de los sistemas para un correcto ingreso de información, el procesamiento correcto de información y la posterior emisión de resultantes en la organización, en este punto se incluyen la evaluación del cumplimiento de funciones actividades y operaciones de empleados, usuarios, funcionarios que estén involucrados con los servicios que son proporcionados por los sistemas computacionales de la organización.

Finalmente, las definiciones utilizadas con anterioridad son las más conocidas y comunes en las auditorías; sin embargo, encontramos la existencia de otras tipologías de auditorías que son especializadas, por ello es muy relevante conocer las conceptualizaciones de dichos modelos, las cuales se presentan a continuación. Con esto, pretendemos fijar los diferentes criterios y unidades especializadas para la evaluación y que existen en materia, de tal manera que los lectores conozcan las tipologías de auditorías y puedan dominarlas en su aplicación. (Muñoz 2013, p.19)

1.3.5 Objetivos generales de la auditoría:

Muñoz (2013), menciona que los objetivos generales de la auditoría son:

Para complementar la conceptualización general, señalaremos muy generalmente los objetivos que pretendemos alcanzar con la auditoría, con la finalidad de que los lectores comiencen a comprender los cimientos sobre las que se desarrollan las auditorías, sea cual estas fuesen. Los objetivos más relevantes son las siguientes:

Poder realizar revisiones independientes de las actividades, funciones o unidades orgánicas especiales en la organización, con el único fin de realizar y emitir un dictamen categórico acerca de la razonabilidad de las operaciones y sus resultantes.

Realizar una revisión específica, dentro de un marco profesional y autónomo, visto desde el aspecto contable, operacional y financiero de las unidades orgánicas del negocio.

Realizar la evaluación del cumplimiento de la planificación, la programación, lineamientos, normativas y políticas que regulan el actuar de los trabajadores y funcionarios de la organización, asimismo apoyar con la evaluación de las actividades desarrolladas en las unidades orgánicas regulares y administrativas.

Informar profesionalmente y con independencia, las resultantes obtenidas por una organización y sus unidades orgánicas, asimismo el desarrollo de las funciones y los cumplimientos de las operaciones y sus objetivos.

Se aclara que todos los objetivos mencionados con anterioridad son de carácter general; no obstante, podrán adecuarse a la tipología de auditoría que se pretende realizar, resultando necesario que previo al inicio de la evaluación de cualquier unidad orgánica, primeramente, se establezcan con precisión los objetivos que pretendemos cubrir con la auditoría, con la finalidad de contar con su difusión, cumplimiento y existencia. (Muñoz 2013, p.29)

1.3.6 Objetivos de la auditoría interna:

Muñoz (2013), presentó los objetivos de las auditorías internas como:

Teniendo en consideración que este tipo de auditorías se pueden realizar con trabajadores que laboran en una misma organización y que este tiene dependencia directa de algún alto funcionario de esta, es muy importante establecer y respetar los objetivos que citaremos a continuación:

Realizaremos evaluaciones que sean independientes dentro de la organización donde se labora, teniendo en cuenta que tienen un mayor conocimiento de las actividades y operaciones, con la finalidad de brindar ayuda en la evaluación del accionar de la gestión administrativa auditada.

Realizar una revisión interna de la unidad orgánica a cargo de la contabilidad, la gestión financiera y del control interno de las unidades de la organización, con la finalidad de realizar su evaluación desde un punto de vista más interno.

Realizar la evaluación interna del cumplimiento de la planificación, programación, políticas, normatividad y lineamientos que regulen el actuar de cada integrante en la organización, asimismo de sus unidades orgánicas administrativas.

Realizar el dictamen de forma interna y relacionada con las operaciones, actividades y funciones que vienen realizándose en la organización, teniendo un mayor conocimiento de las actividades de los trabajadores que laboran en esta, sus funciones y sus tareas. (Muñoz 2013, p.37)

Control:

Según Santillana, tiene por concepto que el control es:

La función de auditoría interna debe ayudar a la organización a mantener un control efectivo mediante la evaluación de la eficiencia y la eficacia de la organización y la promoción de su mejora continua.

2I30.A I- La función de auditoría interna debe evaluar la idoneidad y eficacia de las medidas de control frente a los riesgos de gobernanza y las operaciones y los sistemas de información de la organización, respecto a:

- Alcanzar los objetivos estratégicos de la organización.
- Contabilidad e integridad de la información financiera y operativa.
- La eficiencia y eficacia de las operaciones y planes.
- Proteja los activos.
- Cumplir con las leyes, regulaciones, políticas, procedimientos y compromisos.

2I30.CI- Los auditores internos deben considerar, en la evaluación de los procesos de control de la organización, los conocimientos adquiridos en materia durante sus trabajos de consultoría. (Santillana 2013, p .65)

1.3.7 COBIT 5:

El personal especializado de ISACA® manifestó que:

De manera conceptual se determina que la información es el recurso indispensable (clave) para la totalidad de organizaciones y desde el momento de su creación hasta el momento de su destrucción, es sabido que la tecnología asumió un rol importante. La TI viene avanzando con celeridad, generalizándose en las organizaciones, entornos sociales, de negocio y públicos.

La resultante en consecuencia determina que hoy más que antes, las organizaciones y sus altos ejecutivos invierten sus esfuerzos en:

- La mantención de la información de alto estándar para poder soportar la toma de decisiones del negocio.
- La generación del valor al negocio con inversiones tecnológicas, ejemplo, al alcanzar las metas estratégicas y al generar mayores beneficios al negocio mediante el uso de las TI que vienen siendo eficaces e innovadoras.
- Para lograr la excelencia de sus operaciones mediante aplicaciones tecnológicas eficientes y fiables.

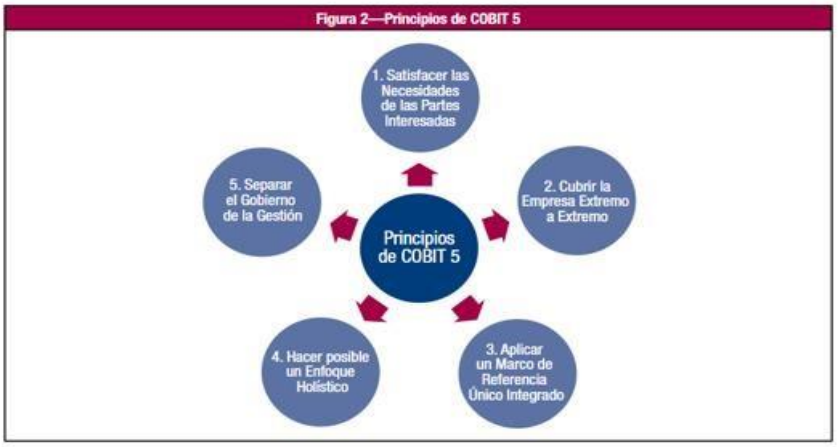
- Lograr la mantención de los riesgos relacionados a las tecnologías en un nivel que se pueda aceptar.
- La optimización de los costes de los servicios tecnológicos.
- Lograr el cumplimiento de las crecientes constantes de leyes, acuerdos contractuales, políticas aplicables y regulaciones.

En el transcurso de la década anterior, la denominación "Gobierno" pasó a la delantera del pensar empresarial como una solución de ejemplos que demostraron la importancia de la buena gobernanza y por el otro de la balanza, a los incidentes de la corporación a nivel global.

Las empresas exitosas reconocen que el comité y los altos ejecutivos tienen que aceptar las tecnologías como cualquiera de sus partes y con la importancia para los negocios. Los comités y la alta dirección (Negocio y TI) deberán colaborar y laborar unidos, con el fin de que se incluyan las TI en los enfoques del gobierno y la gestión. Asimismo, ahora se cuenta con una mayor cantidad de aprobaciones de carácter legal y se vienen implementando regulaciones con el fin de cubrir dicha necesidad.

En el gobierno de TI tenemos marcos de trabajo integrales, entre ellos COBIT 5, la cual sirve de ayuda a las organizaciones para alcanzar sus objetivos de gobierno y gestión de TI corporativas. Explicado de otro modo y más sencillo, permite a las organizaciones contar con la ayuda para la creación del valor óptimo desde las tecnologías alcanzando un equilibrio para generar beneficios y para optimizar los niveles de riesgo y la utilización de recursos. El marco de trabajo integral de COBIT 5 permite a las tecnologías de la información ser gobernadas y gestionadas holísticamente para toda la organización, incluyendo al negocio completamente de principio a fin y las unidades orgánicas funcionales que tienen responsabilidad en las TI, teniendo en cuenta los intereses que las relacionan con TI de las partes de interés internas y externas. El marco de trabajo integral que ofrece COBIT 5 es genérico y útil para organizaciones de cualquier tamaño, comerciales, sin ánimo de lucro o sector público. (ISACA 2012, p.13)

Figura N°1: Principios de COBIT 5



Fuente: ISACA®

Visión General de COBIT 5:

El personal especializado de Isaca ® indicó que:

COBIT 5 proporciona la guía de nueva generación de ISACA para el gobierno y la gestión de las TI en la empresa. Se construye sobre más de 15 años de uso práctico y aplicación de COBIT por parte de muchas empresas y usuarios de las comunidades de negocio, TI, riesgo, seguridad y aseguramiento. Los principales impulsos para el desarrollo de COBIT 5 incluyen la necesidad de:

- Permitir que más partes interesadas expresen sus opiniones para determinar sus expectativas de información y tecnologías relacionadas (qué beneficios pueden obtenerse con niveles de riesgo y costos aceptables) y sus prioridades para garantizar que se entregue realmente el valor esperado. Algunas personas quieren rendimientos a corto plazo, mientras que otras quieren sostenibilidad a largo plazo. Algunas personas estarán dispuestas a correr riesgos, otras no. Estas diferencias, y algunas veces expectativas contradictorias, deben manejarse de manera eficaz. Además, estas partes interesadas no solo quieren involucrarse más, sino que también requieren más transparencia sobre cómo proceder y lograr resultados reales.
- Considere que el éxito de la empresa depende cada vez más de empresas externas y departamentos de TI, como contratistas externos, proveedores, consultores, clientes, servicios en la nube y otros proveedores de servicios, y la dependencia de diversos medios y mecanismos internos para brindar servicios con el valor esperado.
- Manejar la cantidad de información que ha crecido significativamente con el tiempo. ¿Cómo elige la empresa información relevante y confiable para facilitar decisiones comerciales efectivas y eficientes? La información también debe gestionarse de manera eficaz y un modelo de información eficaz puede ayudar a lograr este objetivo.
- Al tratar con la cada vez más común TI, se ha convertido en una parte indispensable de la empresa. Incluso en consonancia con el negocio, tener un departamento de TI independiente por lo general ya no es satisfactorio. Deben ser parte integral de los proyectos empresariales, la estructura organizativa, la gestión de riesgos, las políticas, las tecnologías y los procesos. El rol del director de información (CIO) y el rol de TI están evolucionando. Cada vez más personas en funciones comerciales tienen habilidades de TI y están o estarán involucradas en la toma de decisiones y las operaciones de TI. Las empresas y la TI deberán integrarse mejor.
- Proporcionar otra orientación en las áreas de innovación y tecnologías emergentes. Se trata de creatividad, creatividad, desarrollo de nuevos productos, hacer que los productos existentes sean más atractivos para los clientes y atraer nuevos tipos de clientes. La innovación también implica simplificar el desarrollo de productos, los procesos de fabricación y las cadenas de suministro para aumentar la eficiencia, la velocidad y la calidad para llevar los productos al mercado.

- Cubrir completamente las responsabilidades funcionales de TI y del negocio, y todos los aspectos que llevan a la gestión y el gobierno eficaz de las TI de la empresa, tales como estructuras organizativas, políticas y cultura, además de los procesos.
- Adquirir mejor control sobre soluciones de TI adquiridas y controladas por los usuarios.
- Alcanzar por parte de la empresa:
- Creación de valor a través del uso efectivo e innovador de la TI de la empresa.
- Satisfacción del usuario de negocio con el nivel de compromiso y los servicios de las TI.
- Cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas internas relevantes
- Relaciones mejoradas entre las necesidades de negocio y metas de TI
- Enlazar y, cuando sea relevante, alinearse con otros marcos y estándares principales existentes en el mercado, tales como Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Framework (TOGAF®), Project Management Body of Knowledge (PMBOK®), Projects IN Controlled Environments 2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) y la Organización Internacional de Estándares de normalización (ISO). Esto ayudará a los interesados a entender cómo varios marcos, buenas prácticas y normas están posicionadas respecto al resto y cómo pueden utilizarse juntos.
- Integrar el marco y las directrices principales de ISACA, centrándose principalmente en COBIT, ValIT y RiskIT, y también considerar el Modelo de Negocio de Seguridad de la Información (BMIS), el Marco de Aseguramiento de TI (ITAF), el título de la publicación es Gobierno de TI y Gobernanza Avanzada (TGF) Reunión informativa de la junta para que COBIT 5 cubra todas las actividades comerciales y proporcione una base para integrar otros marcos, estándares y prácticas en un marco.

Sobre la base de la base de conocimiento central de COBIT 5, se desarrollarán diferentes productos y otras pautas para satisfacer las diferentes necesidades de las diferentes partes interesadas, lo que con el tiempo hará que la arquitectura de producto de COBIT 5 sea un documento vivo. La última arquitectura de producto de COBIT 5 se puede encontrar en la página de COBIT del sitio web de ISACA (www.isaca.org/cobit) (ISACA 2012, p .15).

1.3.8 Gestión del Incidente:

Para Morán, la gestión del Incidente lo determina de la siguiente manera:

- Para que un director o ejecutivo de sistemas de información se mantenga permanentemente en su cargo dependerá claramente de que su organización (recurso humano, procesos, etc.) esté preparada y resuelva, grandes crisis, incidentes y peticiones del día a día que ingresan a TI. Si bien es cierto, este no es el único factor crítico, es el más importante y el primero a considerar, ya que de

este dependerá el nivel de confianza que necesite el negocio en relación con las tecnologías.

- Los errores o fallas (incidentes) se presentan como una consecuencia de las operaciones de TI y sus actividades. Estos influyen directamente en el nivel de calidad realizado al desarrollar, los cumplimientos de los lineamientos de las pruebas, la solidez de una arquitectura, que las plataformas sean lo suficientemente robustas, la calidad de técnicos (recurso humano), la solidez o robustez del producto o productos, así como el desempeño de los procesos que la complementan, etc.
- La eficiencia de la gestión de incidentes se concentra en "apagar incendios" de manera inmediata, eliminando los defectos identificados en los servicios, las cuales se debemos corregir en el proceso de la gestión del problema. Mientras que no se logren erradicar todos los errores o fallas, la gestión de incidentes sigue resolviéndolas una tras otra rápidamente, informando además a la gestión de problemas los defectos que identifique en su día a día.

En ese orden de ideas, la gestión de incidentes es el proceso encargado del tratamiento de los sucesos que provocan la degradación o pérdida del normal funcionamiento de un servicio, con el objetivo primordial de recuperar el servicio para el negocio lo más rápidamente posible.

Figura N° 2: Actividades principales del proceso de gestión del incidente

Fuente: ISO 20000

En el marco metodológico de la ISO/IEC 20000 e ITIL v2 o superior, la gestión de incidentes también incorpora los tratamientos para las peticiones o solicitudes de usuarios relacionados con las TI. Para ello, el objetivo primordial es realizar la atención eficientemente y dentro de los plazos acordados. Lamentablemente, este proceso fundamental no se realiza en ninguno de los marcos de metodológicos mencionados.

Suele generar confusión que la gestión de incidentes esté segmentada a su vez en: Gestión de incidentes y Gestión de peticiones. Asimismo, es indispensable clarificar que cuando nos referimos de incidentes o del ciclo de vida de estos, nos referimos al incidente dicho propiamente y no se incluyen las peticiones.

Tuvimos que esperar el lanzamiento de las versiones ITIL v3 o superior para que la gestión de peticiones se reconozca y se trate como un proceso puntual. La demanda de solicitudes de atención por peticiones representa un cargamento significativo de trabajo en los equipos de producción o explotación de las TI, desde ese punto se marca la importancia del desarrollo procedimental y los mecanismos para alcanzar la eficiencia máxima en su atención.

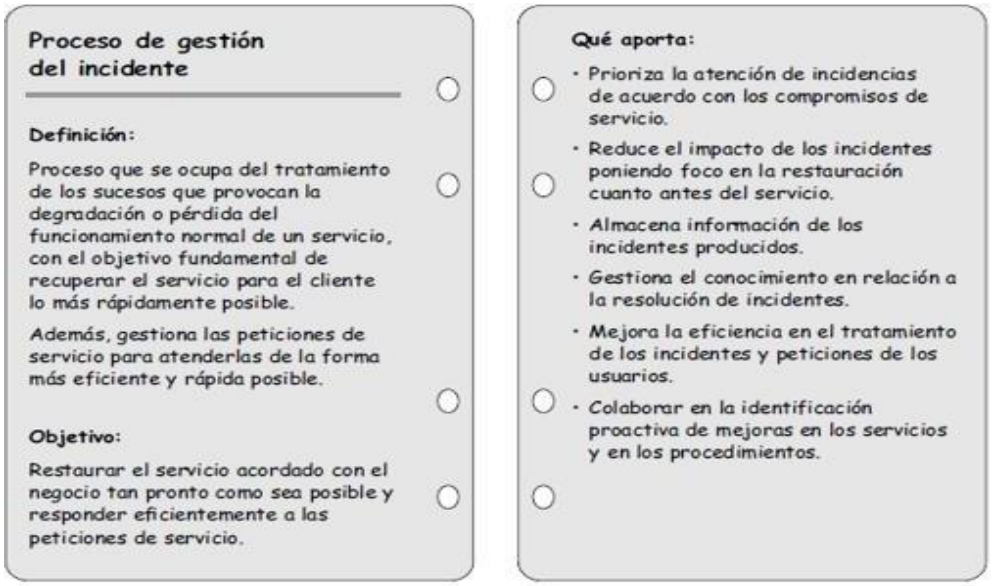
El propósito de una eficiente gestión de incidentes siempre será la de restablecer el funcionamiento normal del servicio, logran la reducción del impacto negativo sobre el negocio, garantizando de este modo, que brindaremos niveles alto de calidad y garantizaremos la disponibilidad del servicio. La operación de los servicios y su correcto funcionamiento dentro de los acuerdos de niveles de servicio, la cual fue sincerada con el negocio para que esta no vea afectación alguna en sus actividades diarias.

Al realizar o brindar servicios no podemos incurrir en aspiraciones mediocres, debemos mantenernos en la búsqueda continua de la mejora de los servicios y que estos no presenten errores o fallas, ya que la aparición de incidente significa la privación de un servicio; por lo tanto, siempre producirá una incomodidad en las actividades de la organización. Por ello, determinamos que los plazos de resolución de incidentes en los SLA (acuerdos de niveles de servicio), serán considerador como limitantes que no deben exceder y por el contrario no deben entenderse como el desempeño máximo de las funciones tecnológicas. (Morán 2009, p.547)

Los objetivos de la gestión del incidente son los siguientes:

- Minimizar el tiempo de resolución de los incidentes.
- Priorizar la atención de incidentes de acuerdo con los compromisos de servicio.
- Reducir el impacto de los incidentes gracias a una resolución oportuna, incrementando de este modo la eficiencia del negocio.
- Contribuir en la identificación de mejoras y modificaciones para los servicios.
- Atender en el tiempo acordado las peticiones de servicio de los usuarios.
- Mejorar permanentemente los procedimientos de atención y resolución, aumentando los niveles de eficiencia en el día a día.
- Lograr la mejora de los indicadores de satisfacción de los usuarios o clientes.

Figura N° 3: Introducción al proceso de gestión del incidente



Fuente: ISO 20000

1.3.9 Las entradas, las actividades y las salidas del proceso:

Morán (2009), clasifica los incidentes de la siguiente manera:

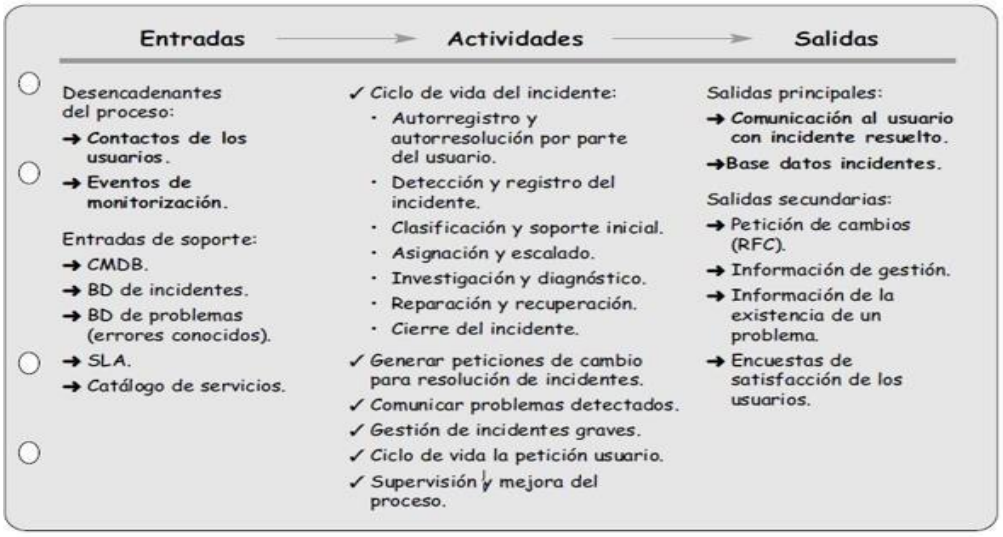
De acuerdo con lo descrito con anterioridad, la gestión de los incidentes contempla dos (2) flujos de actividades:

- Los incidentes y su ciclo de vida.
- Las peticiones y su ciclo de vida.

Estos flujos cuentan con un punto de partida similar en la primera línea de atención de soporte realizado por el Centro de Servicios. Desde aquí, y posterior a su clasificación, se descomponen en dos (2).

Dentro de las actividades realizadas en la gestión de incidentes se encuentra la generación de peticiones de cambio (RFC) las cuales son requeridas para resolver los incidentes, identificación probable de causas recurrentes de incidentes (generando tiques de problemas) y la supervisión evolutiva de los incidentes y la posterior mejora del proceso.

Figura N° 4: Entradas, actividades y salidas del proceso



Fuente: ISO 20000

Las entradas principales de este proceso son:

Contacto de usuarios. Utilizado para comunicar los incidentes, solicitudes, consultas, reclamos o reaperturas de incidentes.

Evento de monitoreo. En este punto se reciben los eventos o alertas procedentes de las herramientas de monitoreo, que es probable que estén relacionados con:

Hardware (Servidores, estaciones de trabajo, impresoras, discos, routers, etc).

Software (Aplicaciones, utilidades, otros sistemas, etc.).

1.3.10 Comunicaciones y telefonía.

Base de datos de la gestión de la configuración (CMDB). De frecuente uso para conocer qué elementos de configuración (CI) pueden estar impactados por un incidente, los servicios impactados y relacionados. Además, se usa para identificar el catálogo de servicios, SLA, autorizaciones de usuarios, documentos, ubicación, etc.

Base de datos de incidentes. Es la base de datos (incidentes) donde se registran y controlan las fases por las que fluyen todos los incidentes. Asimismo, brindan información que permitirá controlar la ocurrencia de más incidentes por la misma causa y poder identificar incidentes pasados y las soluciones que fueron aplicadas.

Base de datos de problemas. Es la base de datos (problemas) utilizada para identificar si un incidente latente provocado por un error conocido y saber la manera de solucionarlo.

Acuerdo de niveles de servicio (SLA). Facilitan información relevante para la priorización de los incidentes y saber el plazo acordado para su resolución.

Dentro de las principales actividades de este proceso podemos dividir estas en relativas a los incidentes, los que se tratan desde el proceso de peticiones y las de mejora. Posteriormente describiremos con más detalle. (Morán 2009, p.554)

Entre las principales salidas del presente proceso se mencionan:

- **Comunicación a usuarios**. Es la información que se traslada al usuario (salida) con el fin de mantenerlo informado en relación al estado del incidente reportado o al final para confirmar su resolución.

- **Base de datos de incidentes**. Es obtenida como salida de una base de datos de incidentes registrados con el tratamiento aplicado.

- **Petición de cambio (RFC)**. Estas son emitidas cuando existe una solicitud con el fin de brindar solución a los incidentes.

- **Información de la gestión**. Es generada la información importante para la gestión y la mejora de los procesos (métricas e indicadores de gestión).

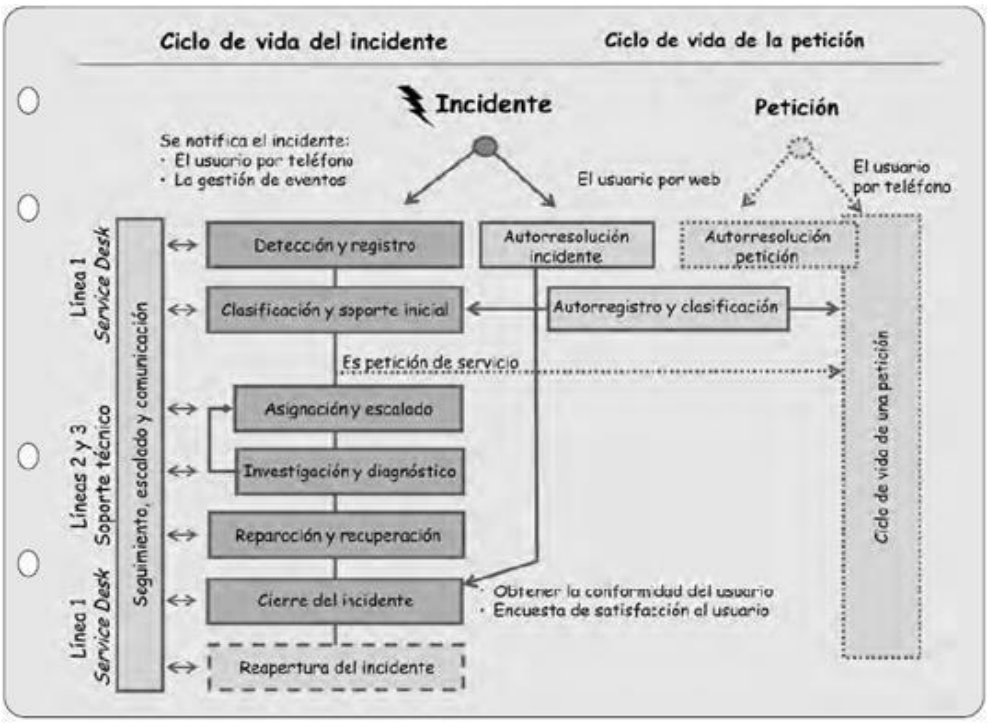
- **Información pre-existente de un problema**. Es trasladada a la gestión de problemas la información referente a probables problemas identificados en el transcurso de las actividades de la gestión del incidente.

- **Encuesta de satisfacción de usuarios**. Se realiza con el cierre de caso de cada incidente

1.3.11 Ciclo de vida de incidentes:

Según Morán (2009), al observar la demanda de actividades asociadas a las tecnologías consideramos que el tratamiento de incidentes, solicitudes y los cambios asociados, son las tres (3) más grandes actividades que requieren en una organización. (Morán 2009, p.555)

Figura N° 5: Ciclo de vida del incidente



Fuente: ISO 20000

1.3.12 Detección y registro del incidente

Según Morán, para detectar y registrar un incidente, menciona lo siguiente:

Como primera actividad en el ciclo de vida de los incidentes se realiza la detección. De manera ideal, estos incidentes deberán ser detectados mediante las herramientas de monitoreo. Sin embargo, por lo general, es el usuario quien realiza la detección o identificación, siendo impactado por este, procediendo posteriormente a informarlo al Service Desk a través de los canales de atención y comunicación de la organización (atención telefónica o registro mediante un aplicativo web).

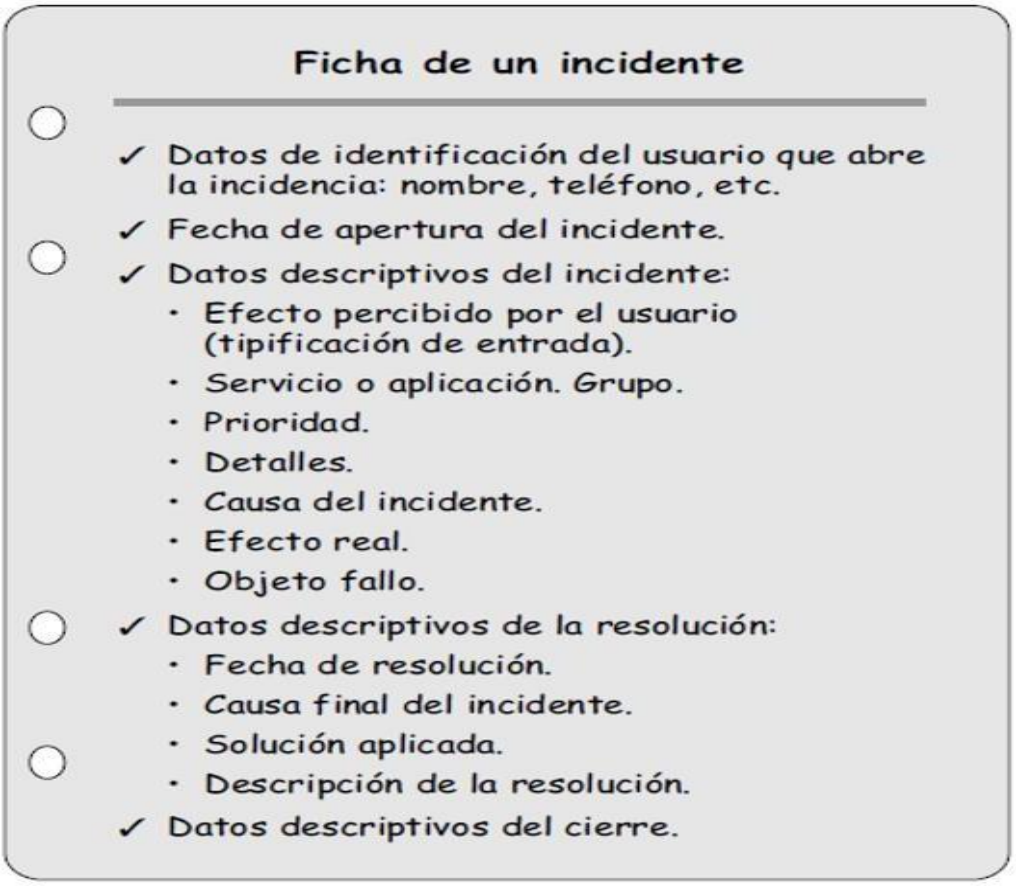
Una vez detectado, el paso siguiente será regístralo en la herramienta de gestión de incidentes. Cabe la posibilidad de registrar un evento (warning), identificada por herramientas de monitoreo, como incidente. El grado de dificultad consistirá en la forma de tratar las alarmas con el fin de discriminar las informativas, las preventivas y las críticas o graves. El monitoreo debe permitir la identificación de un incidente previas al impacto y a los daños que afectan al servicio.

El objetivo primordial de este proceso busca evitar una baja de la calidad del servicio y anticipar un corte. (Morán 2009, p.577)

Las tareas que frecuentemente realizamos en la detección y el registro son las siguientes:

- Validar que el medio de comunicación de los usuarios o de los tiques abiertos automáticamente por el monitoreo corresponden ciertamente a un incidente.
- Realizar un registro preliminar de datos en una ficha o pantalla de registro de incidentes (mediante el agente de atención o por el usuario directo vía web).
- Al tratarse de un incidente, debemos verificar que no haya un registro previo, de darse el caso este debe ser asociado con el incidente existente. De no existir, se guarda como incidente nuevo.
- Al tratarse de una petición o solicitud de servicio o similar, se guarda el registro con la información requerida para su trámite.

Figura N° 6: Ficha o ticket tipo de un incidente



Fuente: ISO 20000

1.3.13 Auto-resolución de usuarios

Según Morán, la auto-resolución de usuarios es:

Esta función ofrece al usuario la posibilidad de resolver un incidente o petición de servicio. De conseguirlo, no será necesario el registro de un tique de atención de incidente.

La atención de auto-resolución es distinta al auto-registro, el cual combina una base de conocimiento (problemas genéricos) de estaciones de trabajo de usuarios, con el

conocimiento obtenido de la organización, relacionada a la configuración del computador o de los servicios.

Asimismo, la auto-resolución suele invocar a las rutinas propias de la empresa, que ejecuta acciones simples asociadas a la resolución de incidentes o su automatización (ejemplo, la eliminación de contraseñas mediante una aplicación).

Con la auto-resolución, se hace indispensable ofrecer a los usuarios la búsqueda de información en la base de datos de conocimiento, el cual permitirá identificar muy fácilmente la solución de su incidente. (Morán 2009, p.558)

1.3.14 Auto-registro y clasificación del usuario

Según Morán, el auto-registro y clasificación del usuario es:

Implementar un formulario web nos resulta tremendamente útil, ya que permite a los usuarios el registro de incidentes y peticiones. De esta manera, se mitiga la demanda de atenciones al centro de atención telefónica en el trabajo de registro, reduciendo drásticamente la cantidad de agentes de atención (tele-operadores). Además, podemos reducir los tiempos de espera en dicho canal de atención (teléfono) a los usuarios atendiéndolos más rápido. Los registros iniciados por los usuarios deben tratarse inmediatamente por el primer nivel de atención y soporte, con el fin de establecer contacto, de necesitarlo, con el usuario. Apenas el usuario este identificado, los datos organizativos (información institucional de su puesto y otros) se deben cargar en la plataforma de atención de manera automática, evitando la introducción repetitiva de la misma información.

Para un auto-registro eficiente es fundamental la disposición de una herramienta que ayude a la clasificación de los casos reportados por los usuarios (incidentes o peticiones), pudiéndose automatizar mejor la primera línea de atención del tique creado.

Relacionado al auto-registro, es conveniente enfocar en la resolución inmediata luego del registro del tique correspondiente, pudiéndose localizar a los usuarios en su unidad orgánica y evitar importantes pérdidas de tiempo en posteriores intentos de contacto.

Tanto la auto-resolución y el auto-registro son importantes para la reducción de la carga de acciones insignificantes a los grupos resolutores de soporte y dan satisfacción a los usuarios permitiéndoles la resolución, por sí mismos, necesidades de manera ágil. Una oportuna mezcla de ambas podría reducir en un 30% el número de contactos (demanda de atención) con el Centro de Servicios. (Morán 2009, p.559)

1.3.15 Clasificación y soporte inicial

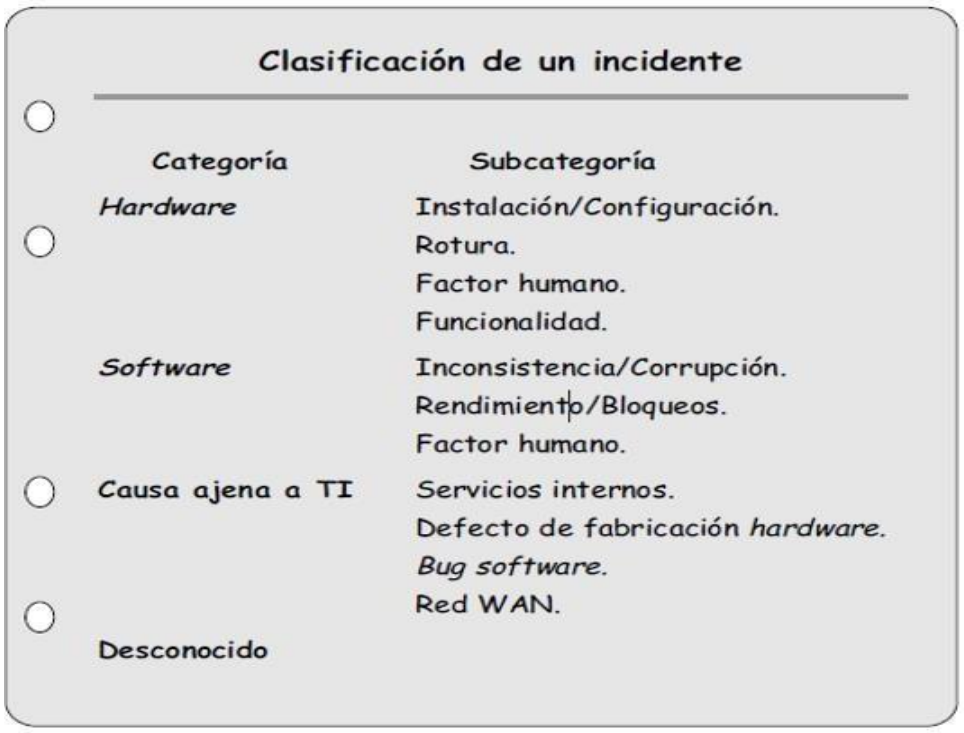
Según Morán, las incidencias se clasifican de la siguiente manera:

Conformada por dos (2) actividades: Clasificación del incidente y dar solución al incidente.

Clasificación. Es la encargada de categorizar el incidente y darle prioridad. Clasificar resulta fundamental para la comparativa automática de los incidentes frente a la base de datos de los problemas y errores conocidos.

La categorización de incidentes tiene como objetivo identificar su origen, los síntomas y las posibles causas (de ser detectadas); esto permitirá identificar fácilmente una solución existente y la asignación a los grupos resolutores de soporte pertinentes.

Figura N° 7: Ejemplo de categorías de un incidente



Fuente: ISO 20000

De acuerdo con ITIL siempre será necesaria la clasificación de los incidentes, peticiones o cambios para los cuales se utilizará la misma estructura (esquema), además se les asignan un orden de importancia, a esta se le denomina prioridad y se le asigna en función de la probabilidad (impacto – urgencia).

Por lo tanto, la prioridad queda establecida en función del:

- **Impacto del negocio**. El término es denominado de esta manera al grado o medida de rigor de un incidente, el cual afecta al negocio (organización o empresa). Frecuentemente las identificamos por el nivel en el que estos incidentes llevan al no cumplimiento de los acuerdos de niveles de servicio. Asimismo, se determina

que el impacto está relacionado con la cantidad de usuarios o sistemas de información afectados.

- **Urgencia**. Es la rapidez solicitada para la resolución de incidentes para un determinado impacto. Por lo general viene determinado por la disponibilidad de tiempo para la resolución de los incidentes sin afectar al servicio brindado.

Por lo regular realizamos una diferenciación en la clasificación al principio del registro de incidentes por el Centro de Servicios, debido a los síntomas y la clasificación final, teniendo en consideración que ya conocemos la causa real. Los incidentes pueden clasificarse para lo largo de su ciclo de vida.

Al momento del cierre será necesario verificar la clasificación por esta información vital para:

- Asociación de incidentes con los elementos de configuración (CI) afectados, usando para esto la CMDB.
- Proporcionar la identificación de incidentes.
- Disponibilidad de data estadística fiable.

- **Soporte inicial**. Con la obtención de la identificación del incidente, trataremos de lograr su resolución de acuerdo a los siguientes pasos secuenciales:
- Debemos comparar el incidente identificado con los incidentes que ya estén registrados en la base de datos de incidentes, corroborando que no existan incidentes relacionados con este y si se cuenta con soluciones ya identificadas. De ser el caso, pasaremos a las actividades descritas para la reparación y recuperación para aplicar la solución que corresponda.
- Debemos comparar con la base de datos de errores conocidos y validar la existencia alternativa de solución que permita resolver el incidente. De encontrarla, se procederá con la actividad de reparación y recuperación del incidente identificado.
- Uso de los conocimientos propios para identificar la mejor solución al incidente.
- En este caso, si identificamos incidentes repetitivos que impacten directamente en los componentes de un servicio, en tal caso generaremos registros para estos problemas. Del mismo modo, notificaremos si no pudiésemos diagnosticar un incidente.
- La atención de soporte técnico inicial culminará cuando este se resuelva o no, sea por falta de conocimiento, medios o por que expiró el plazo de tiempo acordado para su resolución en este canal. De haberlo resuelto se pasará a la fase de reparación y recuperación del incidente. (Morán 2009, p.561)

1.3.16 Asignación y escalamiento

Según Morán, las asignaciones y escalados se clasifican de la siguiente manera:

Si el primer nivel (primera línea de atención) no pudiera resolver un incidente, inmediatamente se lo deberá asignar al segundo nivel resolutor (grupo técnico que corresponde a la segunda línea de atención) cumpliéndose con un escalado

horizontal. Asimismo, si el incidente cuenta con los requisitos definidos, se procederá a informar de manera inmediata a los responsables inmediatos o superiores, cumpliéndose con el escalamiento vertical.

Los escalamientos tienen por objetivo resolver los incidentes lo antes posible, de tal modo que no se incumplan con los acuerdos de niveles del servicio. Los escalamientos pueden ser actividades que pueden ser iterativas y que pueden ser tratados por cualquier grupo de atención de soporte técnico o inclusive por proveedores hasta lograr que se restablezca el servicio.

Existen dos (2) tipologías de escalamiento:

- **Escalamiento funcional**. Consiste en remitir una atención a otro grupo resolutor para continuar trabajando este caso, cuando se requiera incrementar el nivel de especialización que sea necesaria. Es conocida además como escalamiento horizontal. Es realizado por lo general desde los grupos de soporte técnico del primer nivel de atención hacía el grupo resolutor del segundo nivel, o del segundo al tercer nivel. Se resalta la importancia de una correcta tipificación del incidente para lograr que éste sea atendido por el grupo resolutor adecuado.

  Las razones para remitir un escalamiento pueden ser:

  Los grupos de investigación que buscan la resolución del incidente no cuentan con el conocimiento (know how) o experiencia (expertise) necesarios para resolver el incidente. Para este caso, el requerimiento o solicitud vendrá del grupo encargado de la resolución.

  Los tiempos para resolver incidentes disponibles ponen en riesgo el correcto cumplimiento de los acuerdos de niveles de servicio. Para este caso, el escalamiento podría ser también jerárquico.

- **Escalamiento jerárquico**. Consiste en notificar o informar el estado de un incidente de acuerdo con la normativa en gestión de servicios (ISO-20000).

  Las razones para un escalamiento jerárquico son:

  - **La comunicación**. Los tiempos disponibles para la resolución de un incidente puede poner en riesgo el cumplimiento de los acuerdos de niveles de servicio. Este incidente puede ser grave o de alto impacto (significativo) y la alta dirección deben estar informadas. Asimismo, será necesario informar al cliente o usuario en la falta de cumplimiento de los SLA cuando estos se den.

  - **Decisión**. Todos los recursos son importantes y la alta dirección y los usuarios deben estar al tanto del tema. Será necesario tomar decisiones relacionadas a la extensión o aplicación de recursos.

La plataforma de gestión de tiques (herramienta de gestión de incidentes) brinda los medios idóneos para la asignación del incidente entre los grupos de soporte técnico resolutores. La mesa de servicios (Service Desk) supervisará todo el proceso y

controlará mediante alertas o alarmas internas los incidentes que se queden atascados en un grupo o que hayan sido resueltas. (Morán 2009, p.562)

1.3.17 Investigación y diagnóstico de incidentes

Según Morán, la investigación y diagnóstico de incidentes se realiza de la siguiente manera:

El equipo resolutor de soporte técnico que recibe en primera instancia el tique con el incidente asignado realizará las investigaciones de los síntomas y entrega un diagnóstico del incidente, previo a la resolución del incidente. Pese a que la resolución y el diagnóstico estén divididas como actividades independizadas, mayormente para estos casos se realizan en un solo paso.

El grupo resolutor de incidentes encargado, debe investigar usando todos los medios para resolver los incidentes dentro de los tiempos acordados en el procedimiento de escalamiento.

Dentro de esta actividad se realiza lo siguiente:

- El análisis minucioso del incidente.
- Se realiza el análisis y la recopilación de toda la data (información) relacionada.
- La ampliación de la información dentro del registro de los incidentes con los detalles que resulten de la investigación realizada.

Si el grupo de soporte técnico resolutor encargado no tiene la capacidad de resolución del incidente dentro del plazo que le fue asignado, se producirá una nueva asignación y escalamiento. Estas acciones pueden volverse recurrentes e iterativas hasta la resolución del incidente.

Existen riesgos asociados en relación con el personal de soporte técnico, el mismo que puede incurrir en retrasos, dilatando el análisis sin poder ser capaces de controlar los plazos límites de ejecución con los que cuenta en los acuerdos de niveles de servicio, para realizar el escalamiento funcional o jerárquico según corresponda. (Morán 2009, p.563)

1.3.18 Reparación y recuperación del servicio

Según Morán, la reparación y recuperación del servicio se realiza de la siguiente manera:

Con el diagnóstico de la causa de los incidentes ya realizado y encontrada su respectiva solución, temporal o permanente, se procederá con la reparación de la falla. Estas acciones contemplan actividades divididas en tres (3) etapas distintas: La reparación de la falla en el CI (elemento de configuración) impactado, la recuperación inmediata de este CI y la restauración del servicio afectado (reanudación de las operaciones de negocio).

Para la reparación del CI, podría ser necesario contar con los permisos o autorizaciones de la gestión del cambio para aplicar la solución que corresponda. De

acuerdo con la urgencia, realizaremos cambios estándar o realizaremos procedimientos urgentes, generando en estos casos, la solicitud o petición de cambio correspondiente. La resolución de errores no implica necesariamente, que el servicio haya retornado a su normalidad, puesto que igual debemos esperar el reinicio del sistema para que el servicio retorne a su estado de normalidad. Cuando el servicio ya este recuperado, se informará o se pasará el tique a la mesa de servicios (Service Desk).

Desafortunadamente, en el día a día las situaciones no son simples, ejemplo: Una falla puede ocasionar que se corrompa una base de datos o que alguno de sus procesos (batch) se queden por la mitad, el cual debemos reiniciar y terminar; probablemente, tendremos que borrar datos incompletos o debamos repetir desde el principio. Asimismo, será necesario, probablemente, recurrir a las copias de seguridad (respaldo) e informar a los clientes que se perdieron las últimas actualizaciones o facturas.

En definitiva, estas situaciones suelen complicar de manera extraordinaria la solución de un incidente y a su vez generan discusiones acerca del cumplimiento de los acuerdos de niveles de servicio. Ejemplo: Los servicios se pueden recuperar; sin embargo, reparar una base de datos que se haya corrompido puede demorar días o semanas ¿Podríamos decir que un servicio está recuperado una vez que la base de datos está limpia? Si identificamos que falla una cadena de datos, se puede corregir y liberar una nueva versión, pero ¿Se da fin al incidente con esta acción o no culmina hasta que lancemos el trabajo nuevamente y haya finalizado correctamente? Pues bien, el servicio no se puede restablecer por completo hasta que el trabajo de la cadena de datos culmine; pero lo más probable, es que no se pueda lanzar hasta la siguiente noche, aunque el error en la programación en el lenguaje de control de trabajos se solucione rápidamente.

Los resolutores que brindaron la solución a un incidente deberán actualizar el registro de incidentes, completando los detalles propios de la resolución y brindando la información complementaria. (Morán 2009, p.564)

Ejemplo:

- La fecha y hora de resolución del incidente.
- Indicar cuál fue el grupo de soporte técnico que proporcionó la solución.
- Brindar los detalles específicos de la solución.
- Proporcionar los procedimientos y los elementos empleados en la resolución.
- De existir, indicar los incidentes relacionados.

1.3.19 Cierre de incidentes

Según Morán, el cierre de incidentes se realiza de la siguiente manera:

La mesa de servicios (Service Desk) se encarga de la recepción del retorno de tiques de incidentes resueltos, poniendo estas en la lista de tareas que se encuentran pendiente de tratamiento. Este tique será enviado al usuario para obtener su conformidad antes de proceder al cierre correspondiente. Esta conformidad, realizada

normalmente por el usuario, es realizada de manera automática por la herramienta de gestión de incidentes, el mismo que envía un correo electrónico informando la restauración del servicio afectado. Es a partir de este punto que se realizan dos (2) prácticas habituales:

- Solicitar al usuario, de manera expresa, su conformidad mediante correo electrónico o ingresando a la plataforma web de atenciones (herramienta de gestión de incidentes). En el caso de que el usuario no brinde la conformidad o no responda en dos (2) días, este se cerrará de forma automática (no aplicando los niveles de servicio para este caso).
- Ejecutar el cierre automático de todos los incidentes e informar al usuario que existe la posibilidad de reapertura, de no haber conformidad de cierre.

Para los casos de gravedad alta (graves), será recomendable obtener la conformidad directamente del usuario a través de los técnicos que vienen resolviendo los incidentes y están en contacto permanente con ellos, u otra opción, como realizar una llamada telefónica desde la mesa de servicios.

Cuando realicemos la comunicación del cierre de atención (ticket), se acostumbra a anexar una ruta electrónica o enlace url (página web) donde el usuario podrá completar una encuesta breve sobre la atención técnica recibida. La respuesta a esta encuesta es opcional para los usuarios, de este modo lograremos obtener información inmediata de la satisfacción del usuario.

Cuando se toma la decisión de realizar encuestas para usuarios, analizaremos y gestionaremos los resultados que se obtengan, la percepción y las quejas que se manifiesten; sin embargo, es común que esta práctica se utilice solo para obtener métricas periódicas (mensuales o anuales) de satisfacción de usuarios. La mesa de servicios es la encargada del análisis de encuestas de forma regular (por día o semana) y optar por medidas correctivas de manera inmediata.

Una vez que se ha decidido realizar encuestas para usuarios, debemos analizar y gestionar los resultados obtenidos, los comentarios recibidos (percepción) y las quejas que manifiesten. Lamentablemente, es muy común que se utilicen únicamente para conseguir métricas periódicas (mensuales o anuales) de satisfacción del usuario. La mesa de servicios es la encargada de analizar estas encuestas de manera regular (diaria o semanal) y de tomar inmediatamente las medidas adecuadas, según corresponda o realizar las propuestas de mejora que serán incorporadas al plan de mejora general del servicio. Las encuestas que identifiquemos que tengan valoración muy negativa, deberán ser contactadas (el agente deberá llamar inmediatamente al usuario) para conocer los detalles de su punto de vista del servicio recibido; asimismo, es imperativo que podamos restaurar la confianza del usuario en nuestro servicio.

Es de total responsabilidad de la mesa de servicios el cierre manual o automática del incidente.

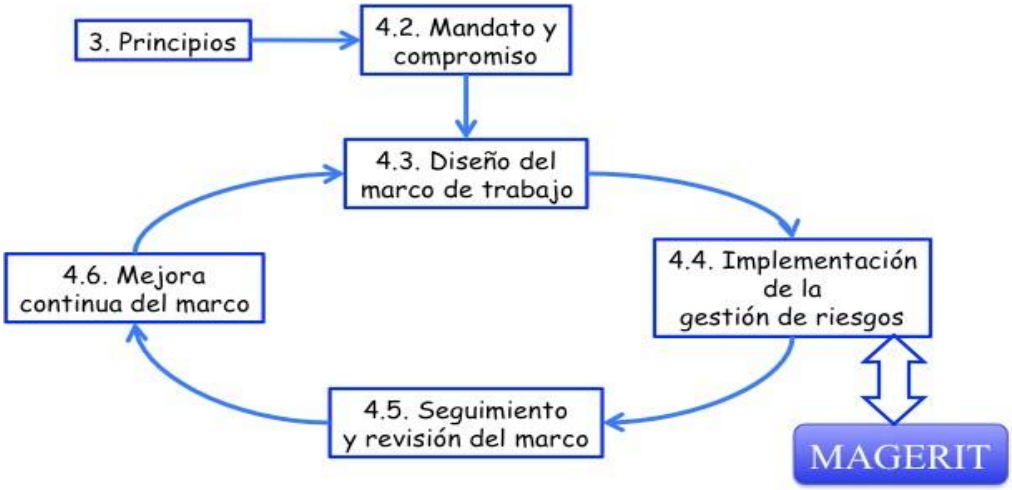
Del cierre de incidentes importantes debemos verificar o validar que el registro del incidente contenga toda la data mínima necesaria y sea anexada la documentación

apropiada. Para el resto de los incidentes, la verificación o comprobación podrá realizarse por una validación informática de los campos en el momento exacto del cierre o por las auditorías periódicas que se realicen a la base de datos de incidentes. (Morán 2009, p.564)

1.3.20 El modelo MAGERIT

Según Amutio (2012), continuando con los términos normativos de la ISO 31000, Magerit es la responsable de la denominación la gestión de riesgos y su gestión, numeral 4.4 "Implementar la gestión de riesgos dentro del marco de gestión de riesgos. En otras palabras, Magerit implementa un proceso de gestión de riesgos dentro de un marco laboral para que las agencias gubernamentales puedan tomar decisiones basadas en los riesgos que plantea el uso de la tecnología de la información. (Amutio 2012, p.07)

Figura N° 8: Proceso de gestión de riesgos



Fuente: ISO 31000

1.3.21 Introducción al análisis y gestión de riesgos

Según Amutio:

La seguridad es la capacidad de una red o sistema de información para resistir accidentes o destruir la disponibilidad, autenticidad, integridad y confidencialidad de los datos y servicios almacenados o transmitidos con cierto grado de resistencia. La red y el sistema proporcionan o hacen accesible. La finalidad de la protección es la misión de la organización, teniendo en cuenta diferentes aspectos de la seguridad:

Disponibilidad

O proporcionar servicios que se utilizarán cuando sea necesario. Disponibilidad insuficiente significa interrupción del servicio. La usabilidad afecta directamente la productividad de la organización.

Integridad

O características que mantienen la integridad y corrección de los datos. Por razones de integridad, la información puede estar alterada, dañada o incompleta. La integridad afecta directamente la correcta ejecución de las funciones organizacionales.

Confidencialidad

O la información solo llega al personal autorizado. Por consideraciones de confidencialidad o confidencialidad, pueden ocurrir fugas y fugas de información y acceso no autorizado. La confidencialidad es una propiedad que es difícil de recuperar y puede destruir la confianza de otros en la organización que no se esfuerzan por mantener la confidencialidad y puede resultar en el incumplimiento de las leyes y compromisos contractuales relacionados con la custodia de datos. Además de la seguridad de estos estándares, se pueden agregar otras herramientas derivadas para acercarnos a la percepción de los usuarios del sistema de información:

Autenticidad

Contiene la identidad o propiedad reivindicada de la entidad o características que garantizan la fuente de los datos. En relación con la autenticidad de la información, podemos manipular la fuente o el contenido de los datos. Con respecto a la autenticidad de los usuarios que acceden al servicio, podemos robar identidades.

Trazabilidad

Asegúrese de poder determinar en todo momento quién hizo qué y cuándo. La trazabilidad es esencial para analizar incidentes, rastrear atacantes y aprender de la experiencia. La integridad del registro de actividad refleja la trazabilidad.

Dependiendo de la situación, todas estas funciones pueden ser necesarias o no. No es obvio simplemente disfrutarlos cuando se necesitan. El esfuerzo y el esfuerzo habituales que tienes que poner para conseguirlos. Los métodos de análisis y gestión de riesgos a partir de la definición están destinados a racionalizar este trabajo.

1.3.22 Riesgo

Estime hasta qué punto la amenaza puede soportar uno o más activos que causan daños o pérdidas a la organización.

El riesgo representa lo que sucederá si el activo no está adecuadamente protegido. Es importante saber en qué características debe enfocarse cada activo y saber en qué medida están en riesgo estas características, es decir, el sistema de análisis:

Análisis de riesgos

El proceso sistemático de estimar la magnitud del riesgo que enfrenta la organización. Sepa que va a pasar, tiene que tomar una decisión

Tratamiento de los riesgos

Proceso destinado a modificar el riesgo.

Hay muchas formas de lidiar con el riesgo: evitar la situación que crea el riesgo, reducir la posibilidad de que ocurra el riesgo, limitar sus consecuencias, compartir con otras organizaciones (generalmente a través de la contratación de servicios o cobertura de seguros), o finalmente aceptar que puede suceder y cuando sea necesario proporcione recursos para actuar. Tenga en cuenta que la opción legal es aceptar el riesgo. A menudo se escucha que no existe una seguridad absoluta. De hecho, siempre debes correr cierto riesgo, es decir, debes conocer y someterte al umbral de calidad exigido para el servicio. Además, a veces aceptamos riesgos operativos para participar en actividades que pueden traernos beneficios más allá de los riesgos o riesgos que estamos obligados a enfrentar. Por eso, a veces se utiliza una definición más amplia de riesgo:

Como todos estos son muy sutiles, no solo son técnicos, sino que también incluyen la decisión de aceptar ciertos riesgos, por lo que debes saber en qué condiciones estás trabajando para poder ajustar la confianza que debe tener el sistema. Por esta razón, es mejor que un enfoque metódico, que puede tomar decisiones informadas y explicar razonablemente las decisiones tomadas (Amutio 2012, p. 10).

1.4 Formulación del problema

1.4.1 Problema general

PG: ¿Cuál será el efecto de la implementación de la auditoría de sistemas en el servicio de atención al usuario en el Ministerio de Educación?

1.4.2 Problemas específicos

PE1: ¿Cuál será el efecto de la implementación de la auditoría de sistemas en el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación?

PE2: ¿Cuál será el efecto de la implementación de la auditoría de sistemas en el diagnóstico de incidentes en el servicio de atención al usuario en el Ministerio de Educación?

PE3: ¿Cuál será el efecto de la implementación de la auditoría de sistemas en la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación?

1.5 Justificación del estudio realizado

1.5.1 La justificación económica

Mediante la realización de este proyecto pretendemos apoyar a la USAU del Minedu, ya que no poseen controles de cumplimiento de procesos y procedimientos para el registro, diagnóstico y resolución de incidencias, el cual colabora en la reducción de la gestión financiera en caso de que estos afecten la imagen institucional; ya que mediante una auditoría basado en el modelo COBIT 5.0 y la metodología de

MAGERIT, nos permitirá tener procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, amenazas y vulnerabilidades que pueda presentar los activos de información.

1.5.2 La justificación tecnológica

Asegurar la continuidad operativa de las plataformas tecnológicas utilizadas por la USAU para el proceso de atención al usuario, instaurando lineamientos para la mejora en la gestión de incidencias basados en el modelo COBIT 5.0 y la metodología de MAGERIT, la cual nos ayudará a realizar matrices de riesgos y tablas de diagnóstico fundamentales para proponer controles de seguridad que mitiguen los daños que pueden afectar los activos de información de la organización auditada.

1.5.3 La justificación institucional

Las medidas de seguridad (controles) que son referidas por el modelo COBIT 5.0 y la metodología de MAGERIT, nos ayudará a resarcir la imagen institucional de la USAU, ya que brindaremos confianza y transparencia a los usuarios con relación al trato de los activos de información, asegurando que estas mantengan su integridad.

1.5.4 La justificación operativa

La realización del proyecto de investigación, así como la implementación de una gestión de servicios eficiente ayudará al tratamiento de incidentes basados en el modelo COBIT 5.0 y la metodología de MAGERIT, permitiendo establecer controles de seguridad y la resolución oportuna del registro, atención y resolución de incidentes que impactan los activos tecnológicos.

1.6 Hipótesis

1.6.1 Hipótesis General

HG: La implementación de la auditoría de sistemas mejora significativamente el servicio de atención al usuario en el Ministerio de Educación.

1.6.2 Hipótesis Específico

HE1: La implementación de la auditoría de sistemas reduce el porcentaje de incidentes asignadas incorrectamente en el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

HE2: La implementación de la auditoría de sistemas reduce el porcentaje de incidentes reclamados en el diagnóstico de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

HE3: La implementación de la auditoría de sistemas reduce el tiempo medio de resolución en la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

1.7 Objetivos

1.7.1 Objetivo General

OG: Determinar el efecto de la implementación de la auditoría de sistemas en el servicio de atención al usuario en el Ministerio de Educación.

1.7.2 Objetivos Específicos

OE1: Determinar el efecto de la implementación de la auditoría de sistemas para el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

OE2: Determinar el efecto de la implementación de la auditoría de sistemas para el diagnóstico de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

OE3: Determinar el efecto de la implementación de la auditoría de sistemas para la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

II. MÉTODO

2.1 Diseño de investigación

Bernal, César manifiesta que los diseños pre-experimentales:

Tienen el más bajo control de variabilidad y no se efectúan asignaciones aleatorias de los sujetos al experimento, siendo estos en los que la persona que realiza la investigación no ejerce control alguno sobre las variables extrañas (no comunes) o intervinientes, no existe asignación aleatoria de los sujetos que participan en la investigación y tampoco hay grupo de control. (Bernal 2010, p.162)

En la realización de la presente tesis utilizaremos el diseño experimental que cuenta con el tipo pre-experimental, teniendo en consideración que manipularemos ambas variables; asimismo, aplicaremos Ishikawa, a través del análisis de dos (2) capas o etapas: Acciones previas (Pre test) y acciones posteriores (Post Test).

Esto permitirá realizar una medición pre-test previa aplicación de auditoría interna, y una medición post-test una vez aplicada la auditoría interna, permitiendo la comparación de ambos resultados y demostrar la hipótesis planteada.

2.2 Variables y operacionalización

2.2.1 Definición conceptual

La variable independiente (VI) para la auditoría de sistemas:

La auditoría interna es una profesión cuyas actividades implican ayudar a las entidades y sus departamentos de gobierno corporativo y administrativo a alcanzar sus objetivos, para lo cual se apoya en una metodología sistemática para analizar los procesos y actividades de negocio y procedimientos relacionados con los grandes retos de la organización. Todo esto conduce a una solución sugerida.

Es una función practicada por auditores internos profesionales con una rica cultura empresarial, conocimiento de sistemas y procesos. Su propósito es brindar seguridad para asegurar que los controles internos apropiados sean suficientes para mitigar los riesgos, y la gestión, control y control de riesgos a través de Auditar, evaluar con resultados cualitativos, cuantitativos, independientes, confiables, oportunos y objetivos con el fin de lograr las metas y objetivos de la organización y gestionar de manera efectiva. Santillana (2013, p .14)

La variable dependiente (VD) para la gestión

Un accidente es una interrupción o reducción no planificada de la calidad de los servicios de TI. La falla de los elementos de configuración que aún no han afectado al servicio también se considera un problema. Van Bon (2011, p .545).

2.2.2 Definición operacional

Auditoría de Sistemas: Son las actividades realizadas por especialistas expertos en la materia (conocimiento del negocio) que busca identificar vulnerabilidades e incumplimientos de planes, procesos, procedimientos, normas y políticas establecidas para el desarrollo continuo en una organización. Estas actividades son realizadas de manera periódica en coordinación con las jefaturas involucradas en el proceso, con la finalidad de aplicar los controles necesarios en beneficio de nuestros usuarios, los cuales utilizan los servicios o productos ofrecidos por la organización.

Gestión: Es el conjunto de actividades que permiten identificar, registrar y tratar los fenómenos que pueden presentar los activos de TI implementados dentro de una organización. Este proceso busca disminuir la recurrencia de las ocurrencias de estos fenómenos, para lo cual, el personal involucrado en el proceso debe registrar y categorizar adecuadamente cada petición o reporte de un cliente o usuario, desde el inicio hasta el fin de la atención (ciclo de vida de la atención), culminando en una evaluación (encuesta de satisfacción) del cliente o usuario.

Tabla N° 1: Tabla de operacionalización de las variables tratadas

Variable	Definición conceptual	Definición operacional	Dimensión	Indicador	Escala
Servicio de atención al usuario	Definida como la conjunción de capacidades organizadas y especializadas que tienen como finalidad la generación de valor para el cliente a través de servicios. (Van Bon 2008, p.27)	Conjunto de actividades que generan valor a una organización en forma de servicios.	Registro	Porcentaje de incidentes asignadas incorrectamente	Razón
			Diagnóstico	Porcentaje de incidentes reclamados	Razón
			Resolución	Tiempo medio de reparación o MTTR	Razón
				D = (Tiempo total transcurrido – Suma de tiempo de inactividad) / Tiempo total transcurrido	

2.3 La población y la muestra

2.3.1 La población

Según Quezada (2010), es la constitución del conjunto de compendios con mayor volumen de donde se puede extraer una muestra que represente el valor experimental científico. (Quezada 2010, p.95)

En el presente proyecto utilizaremos una población que consta de una cantidad de incidentes mensuales, del cual se extrajeron 185 incidentes registrados.

2.3.2 La muestra

Según Quezada (2010), es la elección al azar de un valor cuantitativo de una población, en resumen, es una fracción extraída de la población elegida. (Quezada 2010, p.98)

En el presente proyecto, por conocerse la población tratada, utilizaremos el cálculo de la muestra en base a la fórmula de Quezada.

$$n = \frac{n}{1 + \frac{n_0}{N}}$$

$$n_0 = \frac{Z_a{}^2 \ \sigma^2}{E^2}$$

Dónde:

n: muestra.

n_0: tamaño de muestra aproximado.

N: Tamaño de población bajo Estudio.

Z_α: Valores correspondiente al nivel de significancia.

E: Error de tolerancia de la estimación.

$\sigma^{2:}$ varianza de la variable

Para este tipo de investigación, la muestra será de 126 registros de incidentes en un mes.

2.3.3 El muestreo

Según Quezada (2010), todos los componentes elementales tienen una misma probabilidad al realizar una elección. Los sujetos que serán parte de esta muestra son elegidas al azar a través de numeración aleatoria. En la actualidad sabemos de la existencia de varios métodos que permiten la obtención aleatoria y que son generadas a través de un computador. (Quezada 2010, p.103)

Para obtener el muestreo del presente proyecto de investigación utilizaremos el cálculo de probabilidades (tipo) y simple aleatorio (sub-tipo), ya que nuestros registros de incidentes nos permiten extraer usuarios al azar.

2.4 Técnicas e instrumentos de recolección de datos, confiabilidad y validez

Según Quezada (2010), para que podamos conseguir información realizaremos procedimientos sistemáticos los cuales implicarán a tres (3) actividades que están estrechamente vinculadas entre sí. (Quezada 2010, p.115)

De los cuales tenemos:

- Los instrumentos de medición.
- El equipamiento de medición.
- La codificación de los datos.

2.4.1 Técnicas

La encuesta

Según Bernal (2010), se indica que la encuesta "Aunque ha ido perdiendo credibilidad gradualmente debido al prejuicio de los encuestados, es una técnica de recopilación de información más utilizada". (p.194)

En el presente proyecto de investigación se utilizó la técnica de cuestionario, la cual permitió la recolección de datos del indicador del nivel de compromiso de funciones y responsabilidades.

La observación

Bernal (2010), nos asegura que la presente técnica cobra cada día mayor credibilidad y su uso está generalizándose, esto se debe a que nos permite obtener información directa y confiable, siempre y cuando se realice a través de tareas definidas de manera sistematizada y que tengan control. (Bernal 2010, p.194)

En el presente proyecto de investigación utilizamos la observación para obtener observaciones referentes a los indicadores propuestos.

La entrevista

Según Bernal (2010), se determina que:

Es una técnica para establecer contacto directo con personas que son consideradas directamente como fuentes de información. Existe una diferencia significativa con el cuestionario llenado en el cuestionario; la entrevista puede basarse en un cuestionario flexible diseñado para obtener información pública y espontánea. Mientras tanto, puede profundizar en la información de interés en el caso de estudio. (p.194)

En el presente proyecto se utilizó entrevistas referentes a los inconvenientes y situación de la problemática actual que viene atravesando la USAU**.**

2.4.2 Instrumentos

Encuesta

Según Quezada (2010), el diseño de está:

Inicia con la premisa que, si necesitamos saber más acerca de las conductas de los individuos (usuarios o clientes), es recomendable consultarlo de manera directa. Tratándose finalmente de una solicitud de información a un grupo de personas socialmente significativo en relación a la problemática de estudio para posteriormente realizar un análisis cuantitativo y obtener las conclusiones que correspondan a los datos necesarios. (p.124)

En este proyecto materia de investigación utilizaremos la técnica de la encuesta, con el objetivo de recolectar datos del indicador de tiempo medio de reparación o MTTR.

Entrevistas

Según Quezada (2010), se determina que:

Es un medio específico que implica una interacción puntual y social que tiene como objetivo la obtención de datos para una investigación. La persona que realiza dicha investigación (investigador) realiza preguntas a personas con la capacidad de aportar datos de interés, estableciendo un diálogo particular y peculiar, asimétrico, donde uno de los componentes busca obtener información y la otra viene a ser la fuente de dicha información. (p.124)

Se realizó una entrevista al jefe de la USAU de la OTIC, con el fin de obtener amplia información sobre las problemáticas.

Ficha de observación

Según Quezada (2010), es el registro automatizado, que tiene validez y que el comportamiento o conducta inspira confianza. Asimismo, es identificada como una metodología que la utilizan quienes se orientan conductualmente. (Quezada 2010, p.130)

Los pasos para la construcción de una observación sistematizada son:

- Se definirá con exactitud los aspectos, eventos o las conductas que requieran observación.
- Se extraerá las muestras que representen los aspectos, conductas o eventos que requieran observación.
- Es necesario un repertorio suficiente de conductas que requieran observancia.

- Se deben definir las unidades que requieran observación.
- Se deben definir las categorizaciones y subcategorizaciones de observación.

2.4.3 Validez de los instrumentos

Según Hernández (2006), es el nivel o grado con la que las herramientas o instrumentos miden con precisión las variables necesarias. (Hernández 2006, p.277)

En el presente proyecto que es materia de investigación utilizaremos la validez por contenidos, teniendo en consideración que tomaremos en cuenta el contenido específico con el cual se medirán los instrumentos; por ello, se consultará a los investigadores que estén familiarizados con la variable, considerando su juicio y experiencia (juicio de expertos).

2.4.4 Confiabilidad de los instrumentos

Según Hernández (2006), el componente de confiabilidad de un instrumento de medición es el grado en el cual su aplicación repetida al mismo sujeto u objeto brinda resultados idénticos. (p.277)

Para este proyecto de investigación utilizaremos las fórmulas de coeficiente de variación, se utilizará el Kolmogorov-Smirnov.

2.5 Métodos para el análisis de datos

Para el presente trabajo que es materia de indagación manejaremos los análisis descriptores, los cuales procederán a calcular, su media, medida, tablas y las gráficas de barras o circulares de acuerdo con los resultados y a su vez nos ayudará a realizar un contraste de cada una de las variables que fueron utilizadas.

2.6 Aspectos éticos

La persona que realizará la investigación está comprometida a tratar con respeto la propiedad intelectual, asimismo el derecho de autor, también se respetará la confidencialidad de la información, la cual es brindada por la USAU del Minedu para fines de estudio. Además, se mantiene la confidencialidad de la identidad de las personas o individuos que participaron del proyecto.

III. RESULTADOS

3.1 Análisis Descriptivo

En la presente investigación se pretende implementar la auditoría de sistemas con la finalidad de lograr determinar su efecto en la mejora significativa del Registro, Diagnóstico y Resolución de los servicios de atención al usuario del Minedu, para determinar el efecto, se realizó la evaluación del comportamiento de 126 incidentes, que corresponden a la muestra de la investigación, la cual tiene un tiempo de periodicidad de 30 días hábiles; para ello, se aplicaron las evaluaciones previas para saber la etapa inicial de los tres indicadores; para después, implementar la auditoría de sistemas y nuevamente se proceder con la evaluación de los indicadores en la USAU de la OTIC del Minedu (post test).

Los resultados descriptivos de estas medidas se observan en las tablas 02, 03 y 04.

1° Indicador: Porcentaje de incidentes asignadas incorrectamente.

Tabla N° 2: Medidas descriptoras de incidentes asignadas incorrectamente

En esta tabla se muestran las medidas descriptoras relacionadas al número de incidentes asignadas incorrectamente pre y post de la implementación de la auditoría de sistemas.

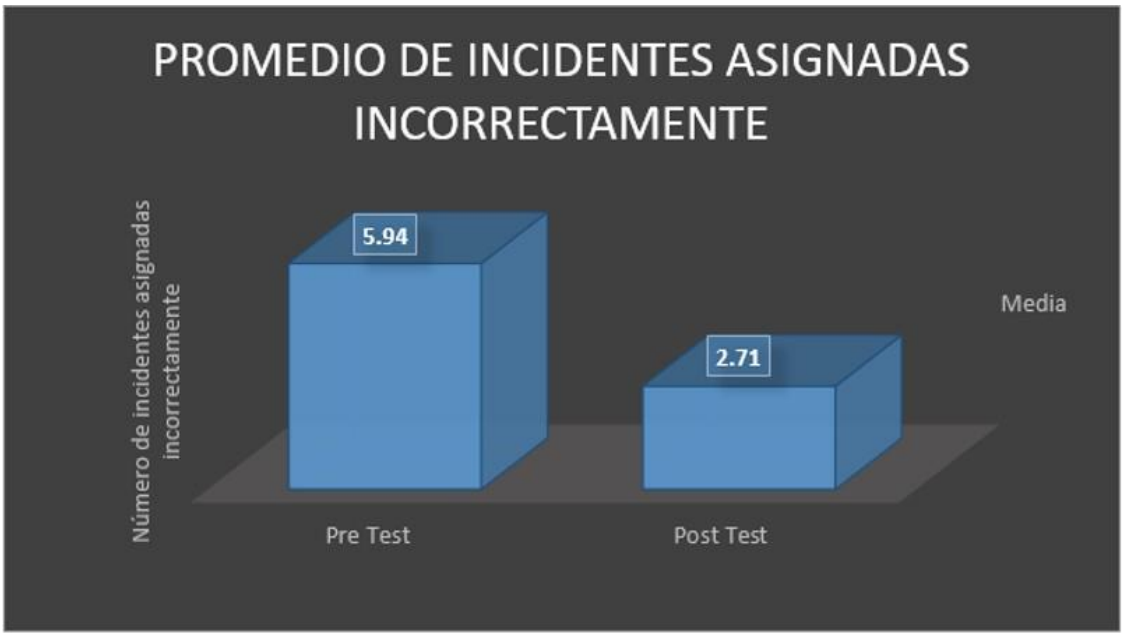
	Media	Mínimo	Máximo	Mediana	Desviación Típica	Coeficiente de Variación
Porcentaje de incidentes asignadas incorrectamente antes	5.94	1	9	6	2.436	0.41%
Porcentaje de incidentes asignadas incorrectamente después	2.71	1	5	3.0	1.220	0.45%

Fuente: Statistical Package for Social Sciences - SPSS

Los valores de media obtenidos de la cantidad de incidentes asignados incorrectamente en la etapa previa de la muestra obtuvieron un valor de 5.94, mientras que en la etapa posterior el número fue de 2.71 de porcentaje de incidentes asignadas incorrectamente, demostrándose que existen diferencias entre lo previo y lo posterior de la implementación de la auditoría de sistemas. Asimismo, el porcentaje mínimo de incidentes asignadas incorrectamente del pre test fueron 1 y el del post test fue 1.

La irradiación del valor cuantitativo de los documentos confidenciales divulgados, en el pre test fue de 0.41% y el post test de 0,45%, validándose que existe gran variabilidad en relación con el resultado no tienen una diferencia significativa; en consecuencia, el comparativo de medias es considerada óptima.

Figura N° 9: Promedio de número de incidentes asignadas incorrectamente antes y después de implementada la Auditoria de Sistemas



Fuente: Sistema de tickets.

2° Indicador: Porcentaje de incidentes reclamados.

Tabla N° 3: Medidas descriptivas del porcentaje de incidentes reclamados

Medidas descriptivas del porcentaje de incidentes reclamados antes y después de la implementación de la auditoría de sistemas.

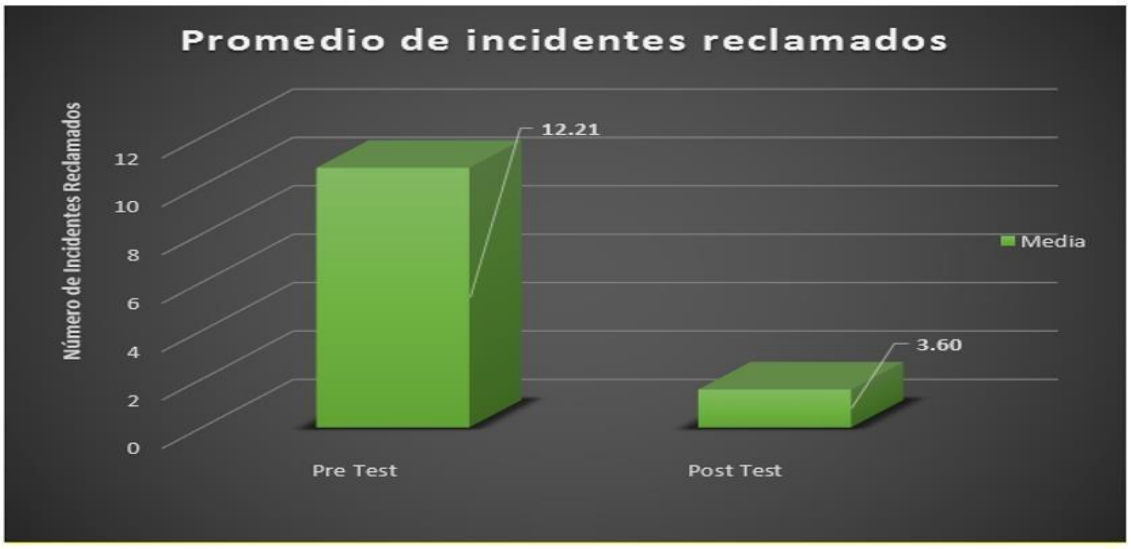
	Media	Mínimo	Máximo	Mediana	Desviación Típica	Coeficiente de Variación
Porcentaje de incidentes reclamados antes	12.21	1	16	12.00	3.35	0.2743%
Porcentaje de incidentes reclamados después	3.60	2	6	4.00	1.195	0.3319%

Fuente: Statistical Package for Social Sciences - SPSS

Se obtuvo como media del porcentaje de incidentes reclamados, en el pre test de la muestra, el valor de 12.21, mientras que para el post test el número fue de 3.60, esto muestra que existe una diferencia entre antes y después de la auditoría de sistemas. Asimismo, el porcentaje mínimo de incidentes reclamados del pre test fueron 1 y en el post test fue de 2.

Lo granular en el porcentaje de incidentes reclamados, en el pretest fue de 3.350% y el post test de 1,195%, podemos observar que esta variabilidad es superior en el pretest; sin embargo, esto no será impedimento para realizar la comparación de medias en ambos momentos.

Figura N° 10: Promedio del número de incidentes reclamados antes y después de la implementación de la Auditoria de Sistemas



Fuente: Sistema de tickets

3° Indicador: Tiempos medios de resolución

Tabla N° 4: Medidas descriptivas del porcentaje de tiempo medio de resolución

Medidas descriptoras del porcentaje de tiempo medio de resolución antes y después de la implementación de la auditoría de sistemas.

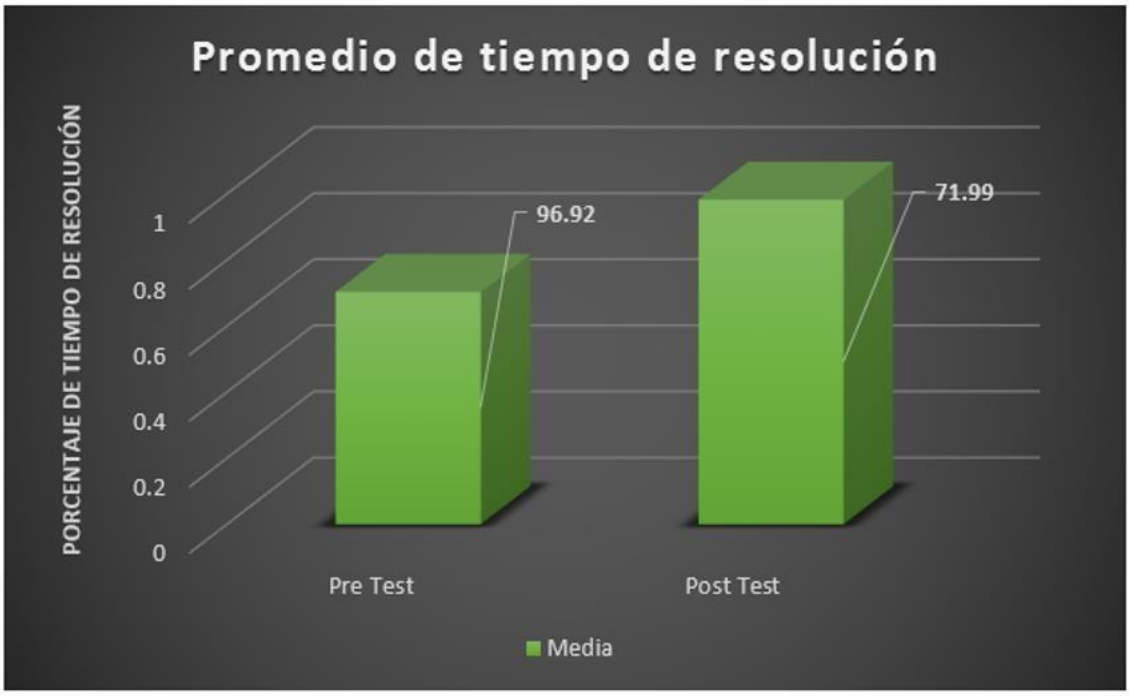
	Media	Mínimo	Máximo	Mediana	Desviación Típica	Coeficiente de Variación
Tiempo medio de resolución antes	96.92	96	98	97	0.683	0.007%
Tiempo medio de resolución antes	71.99	65	76	73	2.603	0.036%

Fuente: Statistical Package for Social Sciences - SPSS

Se obtuvo como media del tiempo medio de resolución del “antes” (pretest) de muestra obteniéndose el valor de 96.92% en la relación al tiempo, por otro lado, el “después” (post test) obtuvo un valor de 71.99%, demostrándose que existe diferencias entre la evaluación previa y posterior a la implementación de la auditoría de sistemas. Además, se obtuvo que el valor porcentual mínimo de tiempo medio de resolución del “antes” fue de 96% y el valor porcentual mínimo del “después” fue de 65%.

La granularidad de valores porcentuales del tiempo medio de resolución en la evaluación previa fue de 0.007% y la posterior de 0.036%, validándose que las variables en relación con los valores obtenidos no presentan grandes diferencias. Por lo tanto, el análisis comparativo de medias es considerado el más adecuado.

Figura N° 11: Porcentaje promedio de tiempo de resolución antes y después de la implementación de la Auditoria de Sistemas



Fuente: Sistema de tickets.

3.2 El análisis inferencial

3.2.1 Prueba de normalización

Para elegir la prueba de hipótesis de este proyecto de investigación, los valores se procesaron mediante una prueba de normalización, con el fin de validar su correcta distribución; en razón a ello, se procedió a realizar la prueba de Kolmogorov-Smirnov a los tres (3) indicadores propuestos, dicha evaluación fue necesidad

prioritaria como media probatoria de normalización y estas fueron aplicadas considerando que las muestras eran grandes.

En ese orden de acciones, para este proyecto de investigación utilizaremos una muestra de 123 incidentes.

1° Indicador: Porcentaje de incidentes asignadas incorrectamente

Con el fin de lograr una determinación para la distribución de los datos planteados para la hipótesis nula (H_o) y la hipótesis alterna (H_a), para posteriormente realizar la comprobación de los datos del número de información confidencial divulgada cuenta con una distribución normal. A continuación, detallaremos las hipótesis planteadas:

$H_{o:}$ Los datos tiene distribución normal.

H_a: Los datos no tienen distribución normal.

Tabla N° 5: Prueba de normalización del valor porcentual de incidentes asignados incorrectamente

La prueba de normalización del valor porcentual de incidentes asignados incorrectamente del "antes" y "después" de la implementación de la auditoría de sistemas.

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
Porcentaje de incidentes asignadas incorrectamente - Antes	0.152	126	0.000
Porcentaje de incidentes asignadas incorrectamente - Después	0.203	126	0.000

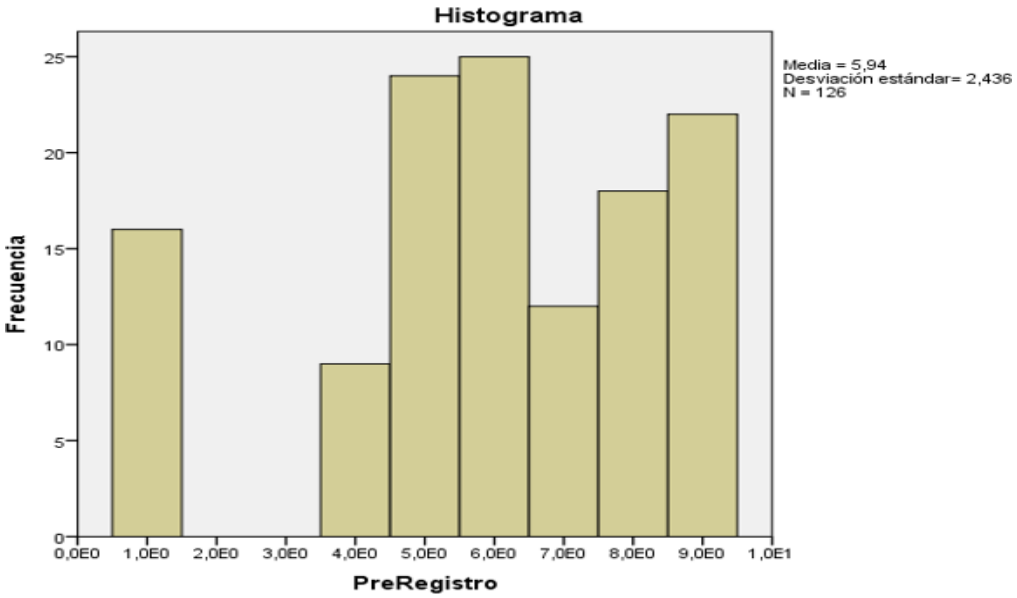
Fuente: Statistical Package for Social Sciences - SPSS

De los valores obtenidos en la prueba se extraen datos que indican que el Sig. de la muestra porcentual de los incidentes asignados incorrectamente en oportunidades anteriores fue de 0.00, entendiéndose que este valor es menor al nivel de significancia alfa (0.05), por lo tanto se rechaza la hipótesis nula, afirmándose entonces que el valor porcentual de incidentes asignados incorrectamente no cumplen con lo requerido en la normalización, el cual se requiere para la aplicación de pruebas paramétricas.

Por otro lado, lo valores resultantes de la prueba señalan que el Sig. de la muestra porcentual de incidentes asignados incorrectamente "después" fue de 0.000, siendo este valor menor que el nivel de significancia alta (0.05); entonces, podemos afirmar que el valor numérico de información no cumple con lo requerido por la normalización.

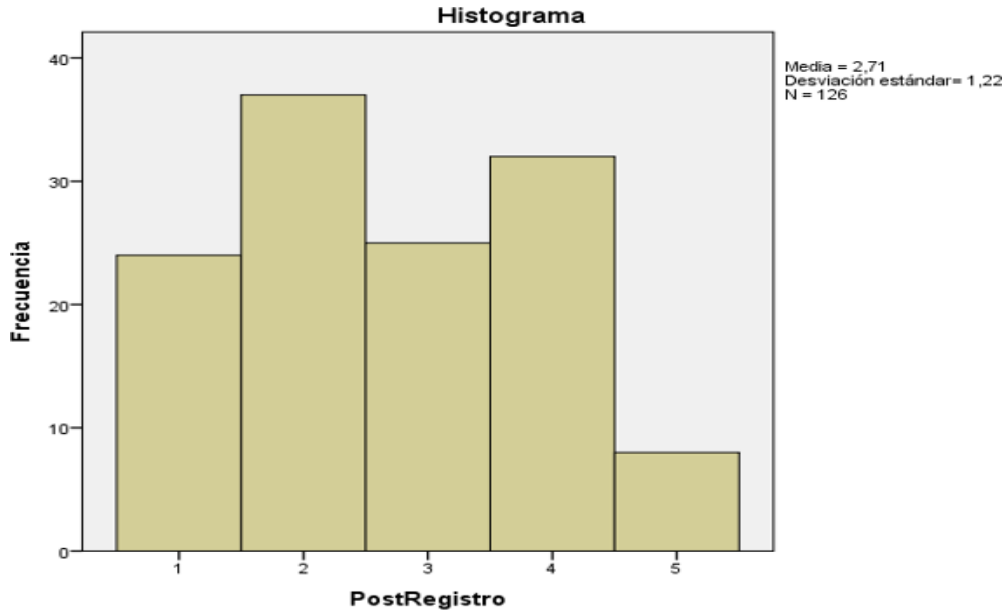
A continuación, se muestran las figuras de distribución de datos, las cuales confirman que esta distribución de datos muéstrales no cumplen con lo requerido en la normalización:

Figura N° 12: Histograma de prueba de normalidad del promedio de número de incidentes asignados incorrectamente antes de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

Figura N° 13: Histograma de prueba de normalidad del promedio de número de incidentes asignados incorrectamente después de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

2° Indicador: Porcentaje de incidentes reclamados.

Para que podamos lograr que se determine la distribución de los datos planteados en la hipótesis nula (H_o), así como en la hipótesis alterna (H_a), para posteriormente comprobar si el valor porcentual de incidentes reclamados cuenta con una distribución regular o normal.

A continuación, detallaremos las hipótesis planteadas:

H_o: Los datos tiene distribución normal.

H_a: Los datos no tienen distribución normal.

Tabla N° 6: Prueba de normalidad del porcentaje de incidentes reclamados

Prueba de normalidad del porcentaje de incidentes reclamados antes y después de implementada la auditoría de sistemas.

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
Porcentaje de incidentes reclamados - Antes	0.296	126	0.000
Porcentaje de incidentes reclamados - Después	0.175	126	0.000

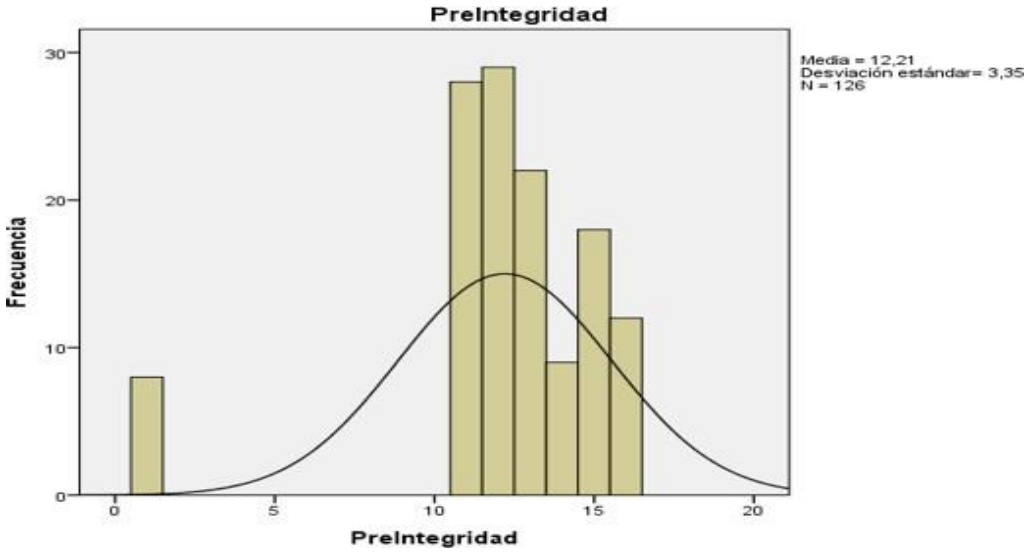
Fuente: Statistical Package for Social Sciences - SPSS

Los valores obtenidos de la prueba nos indican que el Sig. de la muestra porcentual de incidentes reclamados realizadas con anterioridad fueron de 0.0, este valor es menor al nivel de significancia alfa (0.05), entonces rechazaremos la hipótesis nula, entonces evidenciamos que el valor porcentual de incidentes reclamados no cumple el requisito de normalidad.

De otro lado, los valores resultantes de la prueba indican que el Sig. de la muestra del valor porcentual de incidentes reclamados posteriormente es de 0.0, este valor es menor que el nivel de significancia alfa (0.05), concluyéndose que el valor porcentual de incidentes reclamados viene cumpliendo el requisito de normalidad.

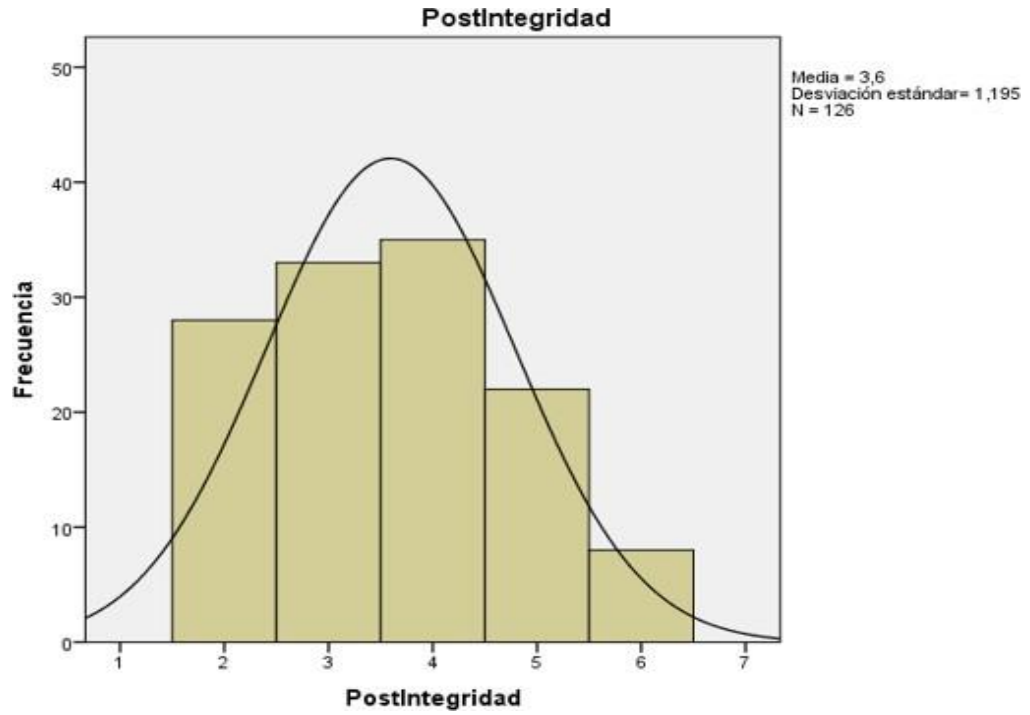
A continuación, se muestran las figuras de distribución de datos, las cuales confirman que esta distribución de datos muéstrales no cumplen con lo requerido en la normalización:

Figura N° 14: Histograma de prueba de normalidad del porcentaje de incidentes reclamados antes de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

Figura N° 15: Histograma de prueba de normalidad del promedio del número o porcentaje de incidentes reclamados después de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

3° Indicador: Tiempo medio de resolución.

Para que podamos determinar cómo se distribuyen los datos trabajados, se realizó el planteamiento de la hipótesis nula (H_o) y así como de la hipótesis alterna (H_a), para posteriormente realizar la comprobación de los datos del tiempo medio de resolución y que estos tienen una normal distribución.

A continuación, detallaremos las hipótesis planteadas:

H_o: Los datos tiene distribución normal.

H_a: Los datos no tienen distribución normal.

Tabla N° 7: Prueba de normalización del tiempo medio de resolución

Dentro de la prueba de normalización (normalidad) del tiempo medio de resolución del "antes" y "después" de la implementación de la auditoría de sistemas.

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
Tiempo promedio de resolución - Antes	0.272	126	0.00
Tiempo promedio de resolución - Después	0.167	126	0.00

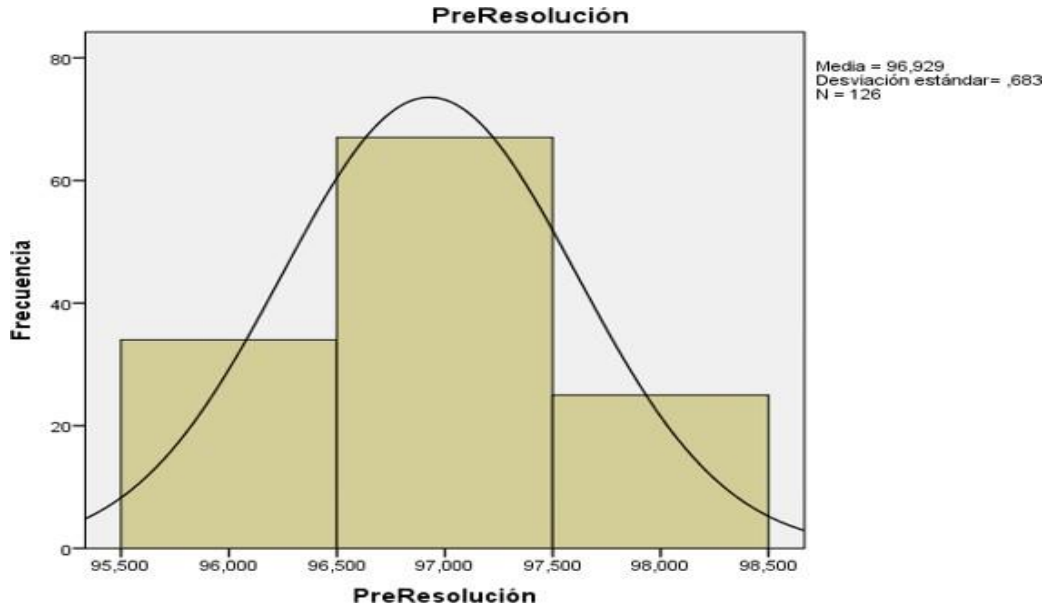
Fuente: Statistical Package for Social Sciences - SPSS

Como resultado de las pruebas realizadas se indican que el Sig. de la muestra del tiempo medio de resolución realizadas con anterioridad fue de 0.00, este valor obtenido es menor que el nivel de significancia alfa (0.05), en conclusión, rechazaremos la hipótesis nula, debido a que los datos no están cumpliendo el requisito de normalidad.

Por otro lado, los valores resultantes de la prueba indican que el Sig. de la muestra del tiempo medio de resolución realizadas posteriormente fue de 0.00, identificando que este valor es menor al nivel de significancia alfa (0.05), donde se indica que los datos no corresponden al cumplimiento del requisito de normalidad.

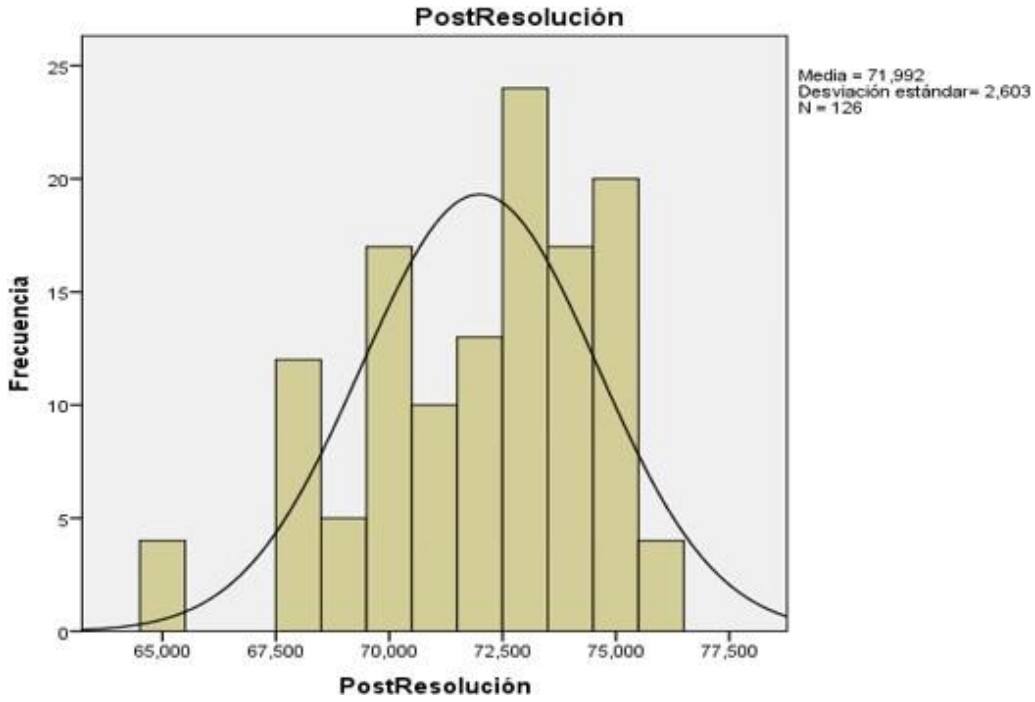
A continuación, se muestran las figuras de distribución de los datos, las cuales confirman que la distribución de estos datos muéstrales no cumplen con lo requerido en la normalización:

Figura N° 16: Histograma de prueba de normalidad en el porcentaje de tiempo medio de resolución antes de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

Figura N° 17: Histograma de prueba de normalidad en el porcentaje de tiempo medio de resolución después de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

3.2.2 Prueba de la hipótesis

De los resultados obtenidos en las pruebas de normalización, quedó demostrado que los indicadores no cumplen con dicho requisito, siendo los valores del "pre test" y "post test" comparados mediante pruebas de rango con la prueba de significancia de Wilcoxon, teniendo un valor de Sig. de 5%.

Hipótesis de investigación N° 01

H1: La implementación de la auditoría de sistemas **mejora significativamente** el servicio de atención al usuario en el Ministerio de Educación.

I1: Porcentaje de incidentes asignadas incorrectamente.

Las hipótesis estadísticas

Definición de variables

$NICD_a$: Porcentaje de incidentes asignadas incorrectamente sin la implementación de la auditoría de sistemas.

$NICD_d$: Porcentaje de incidentes asignadas incorrectamente con la implementación de la auditoría de sistemas.

$H1_0$: La implementación de la auditoría de sistemas no mejora significativamente el registro de la mejora de servicios

$$H1_0: NICD_d \geq NICD_a$$

El indicador de la implementación propuesta es mayor o igual que el indicador actual.

H1a: La implementación de la auditoría de sistemas mejora significativamente el registro de la mejora de servicios.

$$H1_a: NICD_d < NICD_a$$

El indicador de la implementación de la auditoría de sistemas propuesta es menor que el indicador antes de la implementación propuesta.

Tabla N° 8: Pruebas de rango de Wilcoxon del valor porcentual de incidentes asignados incorrectamente

Las pruebas de rango de Wilcoxon para el valor porcentual de incidentes asignados incorrectamente del "antes" y "después" de la implementación de la auditoría de sistemas.

Test	Media	Prueba de Rangos de Wilcoxon	
		Z	Sig. (p)
Porcentaje de incidentes asignadas incorrectamente - Antes	5.94	-8.021	0.000
Porcentaje de incidentes asignadas incorrectamente - Después	2.71		

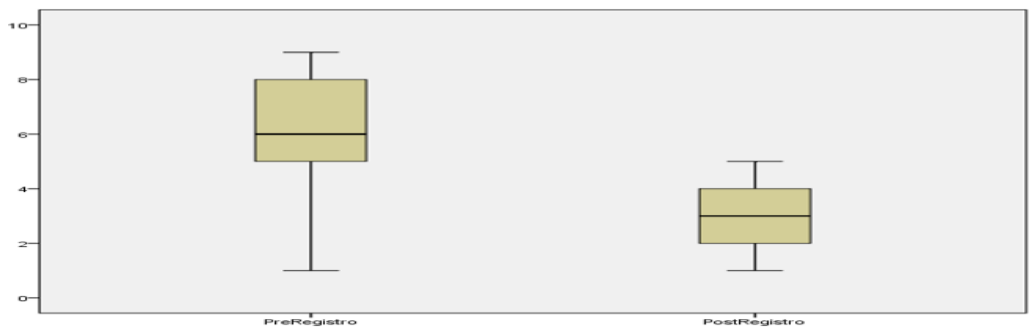
Fuente: Statistical Package for Social Sciences - SPSS

De los valores resultantes de la prueba de rangos de Wilcoxon se muestra que existe una probabilidad de 0.000, la cual es menor a la probabilidad asumida (0.05), con esto podemos rechazar la hipótesis nula, teniendo en cuenta que el valor porcentual de incidentes asignadas incorrectamente del "antes" de la implementación de la auditoría de sistemas resulta significativamente superior al identificado posteriormente a la implementación de esta auditoría.

La figura N° 18, muestra que el Porcentaje de incidentes asignadas incorrectamente es menor en el post test (media = 2.71) en comparación al pre test (media = 5.94); por lo tanto, la implementación de la auditoría de sistemas mejora significativamente el Porcentaje de incidentes asignadas incorrectamente.

Lo cual, se confirma en los resultados de la muestra.

Figura N° 18: Comparación del número de incidentes asignadas incorrectamente antes y después de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

Hipótesis de investigación N° 02

H2: La implementación de la auditoría de sistemas reduce el porcentaje de incidentes reclamados en el diagnóstico de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

I2: Porcentaje de incidentes reclamados.

Hipótesis estadísticas

Definición de variables

$NACNA_a$: Porcentaje de incidentes reclamados sin la auditoría de sistemas.

$NACNA_d$: Porcentaje de incidentes reclamados con la auditoría de sistemas.

$H2_0$: La implementación de la auditoría de sistemas no mejora significativamente la atención al usuario.

$$H2_0: NACNA_d \geq NACNA_a$$

El indicador de la implementación propuesta es mayor o igual que el indicador actual.

H2a: La implementación de la auditoría de sistemas mejora significativamente el diagnóstico de la atención al usuario.

$$H2_a: NACNA_d < NACNA_a$$

El indicador de la implementación de la auditoría de sistemas propuesta es menor que el indicador antes de la implementación propuesta.

Tabla N° 9: Prueba de rangos de Wilcoxon del valor porcentual de incidentes reclamados

Presentamos la prueba de rangos de Wilcoxon del valor porcentual de incidentes reclamados del "antes" y "después" de implementado la auditoría de sistemas.

Test	Media	Prueba de Rangos de Wilcoxon	
		Z	Sig. (p)
Porcentaje de incidentes reclamados - Antes	12.21	-9.680	0.000
Porcentaje de incidentes reclamados - Después	3.60		

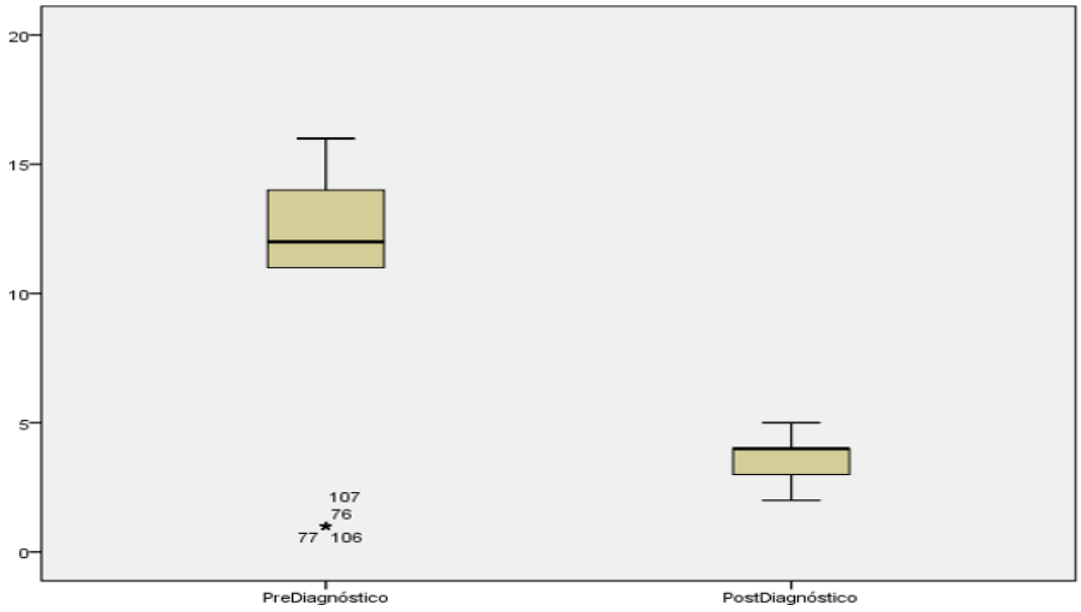
Fuente: Statistical Package for Social Sciences - SPSS

Los valores resultantes de la prueba de rangos de Wilcoxon nos muestran que existe una probabilidad de 0.000, el cual es menor a la probabilidad asumida (0.05), con esto rechazaremos la hipótesis nula, concluyéndose que el valor porcentual de incidentes reclamados "antes" de la implementación de sistemas es mayor al observado "después" de la implementación de la auditoría de sistemas realizada.

La figura N° 19, demuestra que el valor porcentual de incidentes reclamados es significativamente menor en el "pre test" (media = 3.60%), comparado con el "post test" (media = 12.21%) en consecuencia la implementación de la auditoría de sistemas mejora significativamente el porcentaje de incidentes reclamados.

Confirmación de los resultados de la muestra.

Figura N° 19: Comparación del número o porcentaje de incidentes reclamados antes y después de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

Hipótesis de investigación N° 03

H3: La implementación de la auditoría de sistemas mejora significativamente la resolución de la atención al usuario del Ministerio de Educación.

I3: Tiempo medio de la resolución.

Hipótesis estadísticas

Definición de variables

$PTEAS_a$: Tiempo medio de resolución sin implementación de la auditoría de sistemas.

$PTEAS_d$: Tiempo medio de resolución con la implementación de la auditoría de sistemas.

$H3_0$: La implementación de la auditoría de sistemas no mejora significativamente la resolución de la atención al usuario en el Ministerio de Educación.

$$H3_0: PTEAS_a \leq PTEAS_d$$

El indicador actual es menor o igual que el indicador de la implementación propuesta.

H3a: La implementación de la auditoría de sistemas mejora significativamente la resolución de la atención al usuario del Ministerio de Educación.

$$H3_a: PTEAS_d > PTEAS_a$$

El indicador de la implementación de la auditoría de sistemas propuesta es mayor que el indicador antes de la implementación propuesta.

Tabla N° 10: Pruebas realizadas de Wilcoxon en relación con el tiempo medio de resolución

Las pruebas realizadas de Wilcoxon en relación con el tiempo medio de resolución del “antes” y “después” de implementada la auditoría de sistemas.

Test	Media	Prueba de Rangos de Wilcoxon	
		Z	Sig. (p)
Tiempo medio de resolución - Antes	96.928	-9.769	0.000
Tiempo medio de resolución - Después	71.992		

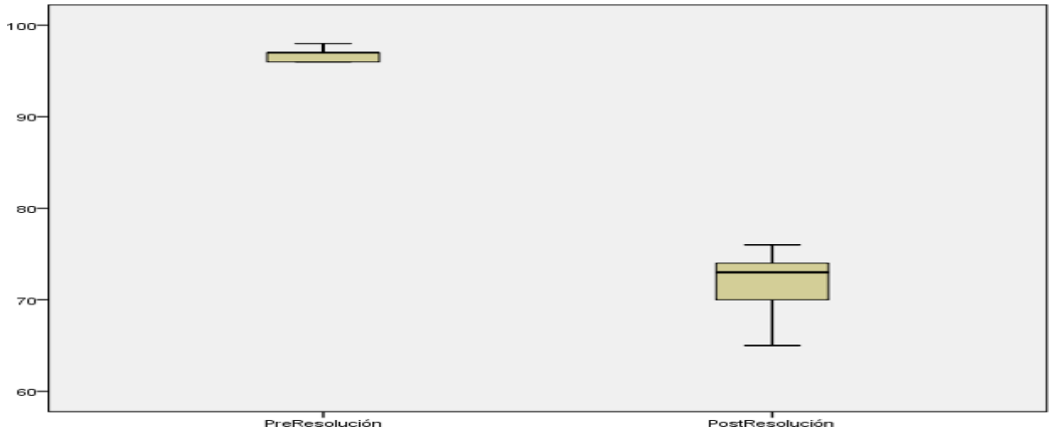
Fuente: Statistical Package for Social Sciences - SPSS

Los valores resultantes de las pruebas aplicadas en los rangos de Wilcoxon nos muestran una probabilidad de 0.000, la cual es menor a la probabilidad asumida (0.05), rechazándose la hipótesis nula, por lo tanto, el tiempo medio de resolución del "antes" de la implementación de la auditoría de sistemas es mucho menor al valor porcentual de tiempo que se encuentra activo el sistema del "después" de dicha implementación.

En la figura N° 25, se muestra que el tiempo medio de resolución es significativamente menor en el "post test" (media = 71.992) en comparativa del "pre test" (media = 96.928); en conclusión, la implementación de la auditoría de sistemas mejora significativamente el tiempo medio de resolución.

Lo cual se confirma en los resultados de las siguientes figuras:

Figura N° 20: Comparación del porcentaje de tiempo medio de resolución antes y después de la implementación de la Auditoria de Sistemas



Fuente: Statistical Package for Social Sciences - SPSS

En relación con el análisis realizado y puesto que se ha demostrado la efectividad de la implementación de la auditoría de sistemas en cada una de las dimensiones de Registro, diagnóstico y resolución en la atención al usuario en el Ministerio de Educación, se puede concluir que la hipótesis general ha sido demostrada y concluyéndose que la implementación de la auditoría de sistemas mejora significativamente la atención al usuario en el Ministerio de Educación.

IV. DISCUSIÓN

Los resultados logrados en el proyecto de investigación permitieron analizar y comparar el número de incidentes asignados incorrectamente, así como el número o porcentaje de incidentes reclamados y el porcentaje de tiempo de resolución del "antes" y "después" de la implementación de la auditoría de sistemas para el servicio de atención al usuario en el Ministerio de Educación.

La cantidad de incidentes asignados incorrectamente, en la prueba de medición del "pre test" se alcanzó hasta un promedio porcentual de 5.94% de incidentes asignadas incorrectamente; sin embargo, al realizar la implementación de la auditoría de sistemas el valor se redujo a 2.71%. De los resultados obtenidos se observa que hubo una reducción de 3.23% de incidentes asignados incorrectamente, pudiéndose afirmar que al realizar la implementación de la auditoría de sistemas se logró una reducción del valor porcentual equivalente al 54%.4% del número de incidentes asignadas incorrectamente en la USAU de la OTIC del Minedu.

Según la investigación realizada por Agramonte (2016), se demostró que el 38% de los trabajadores encuestados expresaron que la actual seguridad lógica se encontraba en un nivel 1 – Inicial; el 69% de los trabajadores encuestados indicaron que la seguridad de las aplicaciones están en un nivel 3 – definido y por último el 55% de los trabajadores encuestados refirieron también en el nivel 3 – definido para la actual administración del centro de procesamiento de datos.

El número de incidentes reclamados al realizar la medición del "pre test" alcanzó un valor porcentual de 12.21% de incidentes reclamados y al realizar la implementación de la auditoría de sistemas, este se redujo a 3.60%. El valor porcentual resultante obtenidas, muestran que se logró una reducción del 8.61% de incidentes reclamados; concluyéndose que, se puede afirmar que con la auditoría de sistemas logramos una reducción porcentual del 70.5% en el número de incidentes reclamados en la USAU de la OTIC del Minedu.

Según la investigación elaborada por Gago (2013), se comprobó que el 95% de los encuestado está de acuerdo con la implementación de una oficina de auditoría interna como un alternativa para evaluar el accionar de las cooperativas de servicios múltiples de Lima Metropolitana; Asimismo, el 85% de encuestados están de acuerdo que es importante el diagnostico interno (auditoría) para evaluar la operación de las cooperativas auditadas; el 95% de encuestados están de acuerdo con los productos de la eficiente administración de los recursos en las cooperativas y finalmente el 100% de encuestados está de acuerdo que la toma de decisiones oportuna es trascendental para el logro de objetivos en estas cooperativas.

El valor porcentual del tiempo de resolución, al realizar la medición del "pre test" se alcanzó un promedio de 96.92% de tiempo medio de resolución y posteriormente a la implementación de la auditoría de sistemas reducimos el valor porcentual a 71.99%. Estos valores resultantes obtenidos nos muestran que existe una reducción del 24.93% en el tiempo medio de resolución, es así que podemos afirmar que al implementar la auditoría de sistemas se logra una reducción del 25.72% del tiempo medio de resolución en la USAU de la OTIC del Minedu.

Según el trabajo de investigación realizada por Huamán (2014), se demuestra que existe un cumplimiento cuantitativo en la empresa del estado peruano, obteniéndose un valor porcentual de 91.66% del dominio 5 y un valor porcentual de 83.33% del dominio 7, enmarcados en la "NTP-ISO/IEC 17799:2007" como parte del proceso que implementaremos con el referente de la "NTP-ISO/IEC 27001:2008 – Sistema de Gestión de Seguridad de la Información".

V. CONCLUSIONES

De la investigación y el análisis realizado se obtuvieron las siguientes conclusiones:

Primera: Queda demostrado que una implementación de auditoría de sistemas reduce la cantidad de incidentes asignadas incorrectamente, la cual nos permitió lograr la demostración de las hipótesis planteadas con una reducción porcentual del 54.4% en el registro de incidentes para el servicio de atención al usuario en el Ministerio de Educación, y esta se vio reflejada al incrementar los grados de nivel de satisfacción de los usuarios.

Segunda: Queda demostrada que al realizar la implementación de la auditoría de sistemas se logra reducir la cantidad de incidentes reclamados, el logro obtenido nos demuestra las hipótesis planteadas con una reducción porcentual del 70.5% en el diagnóstico de incidentes para el servicio de atención al usuario en el Ministerio de Educación, y esta se ve reflejada al incrementar los grados de satisfacción de los usuarios.

Tercera: Se ha determinado que al implementar la auditoría de sistemas se reduce el tiempo medio de resolución, pudiéndose demostrar que la hipótesis planteada con una reducción porcentual del 22.75% en la resolución de incidentes para el servicio de atención al usuario en el Ministerio de Educación, y esta se ve reflejada al incrementar los grados de satisfacción de los usuarios.

VI. RECOMENDACIONES

Primera: Recomendamos implementar un equipo de trabajo con la función de velar por la Calidad de Servicios de TI que se encargue del cumplimiento y seguimiento de los procesos y procedimientos establecidos por la Unidad de Servicio de Atención al Usuario – USAU de la OTIC del Minedu.

Segunda: Se recomienda la implementación de canales de atención para Quejas, Reclamos y Sugerencias, mediante el cual se atienda al usuario ante un incumplimiento de servicio.

Tercera: Se recomienda que las auditorías internas se realicen de manera periódica, con la finalidad de asegurar el cumplimiento de los procesos y procedimientos elaborados e implementados por la Unidad de Servicio de Atención al Usuario de la OTIC del Minedu.

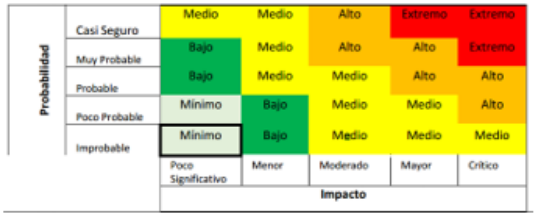
VII. REFERENCIAS

- Amutio, Miguel A. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España: © Ministerio de Hacienda y Administraciones Públicas.
- Bernal, César A. (2002). Metodología de la investigación. Tercera edición. Colombia: Pearson Educación.
- Hernández, Roberto. (2006). Metodología de la investigación. Cuarta Edición. México: McGraw-Hili Interamericana.
- Montaño Ardila, Víctor. Combita Niño, Harold. De La Hoz Franco, Emiro. (2016). Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Practicas TI en cumplimiento de la Ley Sarbanes–Oxley. Diciembre 2016, de Revista Espacios.
- Morán Abad, Luis. (2009). Guía completa de aplicación para la gestión de los servicios de tecnologías de la información. España: AENOR.
- Muñoz Razo, Carlos. (2002). Auditoria en sistemas computacionales. México: Pearson Educación.
- Quezada Ramón, Alberto. Martínez Reyes, Fray. Cazar Ramírez, María Elena. (2010). Metodología de la investigación. Octubre 2009, de Universidad de Azuay, Facultad de Medicina.
- Santillana González, Juan Ramón. (2013). Auditoria interna. México: Pearson Educación.
- Van Bon, Jan. (2008). Operación del servicio basada en ITIL V3 - Guía de Gestión. Holanda: CO2 Premedia.

VIII. ANEXOS

8.1 Anexo N° 1: Ficha de revisión de hallazgos de vulnerabilidades

PERÚ | Ministerio de Educación | Secretaría de Planificación Estratégica | Oficina de de Tecnologías de la Información y Comunicación | Unidad de Sistemas de Información

	REPORTE DE HALLAZGOS					
	ESPECIALISTA DE CYA					
	FECHA Y HORA DE REVISIÓN					
	NOMBRE DEL HALLAZGO					
	PLATAFORMA					
	DESCRIPCIÓN DEL HALLAZGO					
SEGURIDAD	**ANALISIS DE RIESGOS**					
	DEPENDENCIAS					
	CONEXIONES A INTERNET	**Acción**	**Proceso**	**Destino**	**Comentario**	
	ANALISIS					
	RECOMENDACIÓN					

Formato V. 1 Elaboración Propia Página 1

8.2 Anexo N° 2: Ficha de observación

FORMATO PRE Y POST TEST		
ÍTEM: Porcentaje de incidentes asignadas incorrectamente		
DIMENSIÓN: Registro		
Ministerio de Educación - Unidad de Servicios y Atención al Usuario - OTIC		
REGISTRO	**Porcentaje de incidentes asignadas incorrectamente**	
	PRE TEST	**POS TEST**
1	0.09	0.04
2	0.1	0.04
3	0.06	0.03
4	0.05	0.02
5	0.1	0.05
6	0.1	0.04
7	0.09	0.04
8	0.04	0.04
9	0.07	0.05
10	0.04	0.02
11	0.05	0.03
12	0.08	0.04
13	0.08	0.04
14	0.05	0.03
15	0.06	0.03
16	0.07	0.02
17	0.1	0.03
18	0.05	0.02
19	0.08	0.02
20	0.06	0.02
21	0.06	0.03
22	0.06	0.01
23	0.09	0.02
24	0.05	0.02
25	0.09	0.01
26	0.05	0.01
27	0.06	0.02
28	0.09	0.01
29	0.08	0.01
30	0.07	0.01
31	0.07	0.05
32	0.1	0.04

33	0.06	0.03
34	0.06	0.03
35	0.1	0.05
36	0.1	0.04
37	0.09	0.04
38	0.04	0.04
39	0.09	0.04
40	0.04	0.02
41	0.05	0.03
42	0.08	0.04
43	0.08	0.04
44	0.05	0.03
45	0.05	0.02
46	0.07	0.02
47	0.1	0.03
48	0.05	0.02
49	0.08	0.02
50	0.06	0.02
51	0.06	0.03
52	0.06	0.01
53	0.09	0.02
54	0.05	0.02
55	0.09	0.01
56	0.05	0.01
57	0.06	0.02
58	0.09	0.01
59	0.08	0.01
60	0.07	0.01
61	0.07	0.05
62	0.1	0.04
63	0.06	0.03
64	0.06	0.03
65	0.1	0.05
66	0.1	0.04
67	0.09	0.04
68	0.04	0.04
69	0.09	0.04
70	0.04	0.02
71	0.05	0.03
72	0.08	0.04
73	0.08	0.04
74	0.05	0.03

75	0.05	0.02
76	0.07	0.02
77	0.1	0.03
78	0.05	0.02
79	0.08	0.02
80	0.06	0.02
81	0.06	0.03
82	0.06	0.01
83	0.09	0.02
84	0.05	0.02
85	0.09	0.01
86	0.05	0.01
87	0.06	0.02
88	0.09	0.01
89	0.08	0.01
90	0.07	0.01
91	0.07	0.05
92	0.1	0.04
93	0.06	0.03
94	0.06	0.03
95	0.1	0.05
96	0.1	0.04
97	0.09	0.04
98	0.04	0.04
99	0.09	0.04
100	0.04	0.02
101	0.05	0.03
102	0.08	0.04
103	0.08	0.04
104	0.05	0.03
105	0.06	0.02
106	0.07	0.02
107	0.1	0.03
108	0.05	0.02
109	0.08	0.02
110	0.06	0.02
111	0.06	0.03
112	0.06	0.01
113	0.09	0.02
114	0.05	0.02
115	0.09	0.01
116	0.05	0.01

117	0.07	0.02
118	0.09	0.01
119	0.08	0.01
120	0.09	0.01
121	0.04	0.04
122	0.09	0.04
123	0.06	0.02
124	0.05	0.03
125	0.08	0.04
126	0.08	0.04
Totales	8.92	3.41

Fuente: Formato pre y post test del porcentaje de incidentes asignadas incorrectamente

FICHA DE OBSERVACIÓN

FORMATO PRE Y POST TEST		
ITEM: Porcentaje de incidentes reclamados		
DIMENSIÓN: Diagnóstico		
Ministerio de Educación - Unidad de Servicios y Atención al Usuario - OTIC		
REGISTRO	**Porcentaje de incidentes reclamados**	
	PRE TEST	**POS TEST**
1	0.15	0.06
2	0.11	0.06
3	0.11	0.05
4	0.12	0.05
5	0.15	0.05
6	0.11	0.04
7	0.16	0.04
8	0.12	0.04
9	0.15	0.04
10	0.15	0.04
11	0.14	0.05
12	0.13	0.04
13	0.13	0.05
14	0.12	0.03
15	0.11	0.03
16	0.1	0.03
17	0.1	0.04
18	0.11	0.03
19	0.13	0.03
20	0.14	0.03

21	0.11	0.04
22	0.16	0.03
23	0.16	0.02
24	0.13	0.02
25	0.13	0.02
26	0.12	0.02
27	0.12	0.03
28	0.11	0.02
29	0.12	0.02
30	0.12	0.02
31	0.11	0.06
32	0.15	0.06
33	0.11	0.05
34	0.12	0.05
35	0.15	0.05
36	0.11	0.04
37	0.16	0.04
38	0.12	0.04
39	0.15	0.04
40	0.15	0.04
41	0.14	0.05
42	0.13	0.04
43	0.13	0.05
44	0.12	0.03
45	0.11	0.03
46	0.1	0.03
47	0.1	0.04
48	0.11	0.03

49	0.13	0.03
50	0.14	0.03
51	0.11	0.04
52	0.16	0.03
53	0.16	0.02
54	0.13	0.02
55	0.13	0.02
56	0.12	0.02
57	0.12	0.03
58	0.11	0.02
59	0.12	0.02
60	0.12	0.02
61	0.11	0.06
62	0.15	0.06
63	0.11	0.05
64	0.12	0.05
65	0.15	0.05
66	0.11	0.04
67	0.16	0.04
68	0.12	0.04
69	0.15	0.04
70	0.15	0.04
71	0.14	0.05
72	0.13	0.04
73	0.13	0.05
74	0.12	0.03
75	0.11	0.03
76	0.1	0.03

77	0.1	0.04
78	0.11	0.03
79	0.13	0.03
80	0.14	0.03
81	0.11	0.04
82	0.16	0.03
83	0.16	0.02
84	0.13	0.02
85	0.13	0.02
86	0.12	0.02
87	0.12	0.03
88	0.11	0.02
89	0.12	0.02
90	0.12	0.02
91	0.11	0.06
92	0.15	0.06
93	0.11	0.05
94	0.12	0.05
95	0.15	0.05
96	0.11	0.04
97	0.16	0.04
98	0.12	0.04
99	0.15	0.04
100	0.15	0.04
101	0.14	0.05
102	0.13	0.04
103	0.13	0.05
104	0.12	0.03

105	0.11	0.03
106	0.1	0.03
107	0.1	0.04
108	0.11	0.03
109	0.13	0.03
110	0.14	0.03
111	0.11	0.04
112	0.16	0.03
113	0.16	0.02
114	0.13	0.02
115	0.13	0.02
116	0.12	0.02
117	0.12	0.03
118	0.11	0.02
119	0.12	0.02
120	0.12	0.02
121	0.15	0.04
122	0.15	0.04
123	0.14	0.05
124	0.13	0.04
125	0.13	0.05
126	0.12	0.03
Totales	16.1	4.53

Fuente: Formato pre y post test del porcentaje de incidentes reclamados

FICHA DE OBSERVACIÓN

FORMATO PRE Y POST TEST DEL INDICADOR TIEMPO MEDIO DE LA REPARACIÓN O MTTR		
FÓRMULA: D = (tiempo total transcurrido – suma de tiempo de inactividad) / tiempo total transcurrido		
DIMENSIÓN: Resolución		
Ministerio de Educación - Unidad de Servicios y Atención al Usuario - OTIC		
REGISTRO	**Tiempo medio de reparación o MTTR**	
	PRE TEST	**POS TEST**
1	0.98	0.65
2	0.98	0.75
3	0.97	0.73
4	0.96	0.74
5	0.96	0.73
6	0.97	0.72
7	0.97	0.74
8	0.96	0.74
9	0.97	0.72
10	0.98	0.71
11	0.97	0.71
12	0.96	0.70
13	0.97	0.69
14	0.97	0.70
15	0.98	0.75
16	0.97	0.73
17	0.96	0.72
18	0.97	0.74
19	0.97	0.75

20	0.98	0.76
21	0.97	0.70
22	0.96	0.68
23	0.97	0.70
24	0.97	0.68
25	0.98	0.75
26	0.97	0.73
27	0.96	0.73
28	0.96	0.68
29	0.97	0.75
30	0.97	0.73
31	0.98	0.75
32	0.98	0.65
33	0.97	0.73
34	0.96	0.74
35	0.96	0.73
36	0.97	0.72
37	0.97	0.74
38	0.96	0.74
39	0.97	0.72
40	0.98	0.71
41	0.97	0.71
42	0.96	0.70
43	0.97	0.69
44	0.97	0.70
45	0.98	0.75
46	0.97	0.73
47	0.96	0.72

48	0.97	0.74
49	0.97	0.75
50	0.98	0.76
51	0.97	0.70
52	0.96	0.68
53	0.97	0.70
54	0.97	0.68
55	0.98	0.75
56	0.97	0.73
57	0.96	0.73
58	0.96	0.68
59	0.97	0.75
60	0.97	0.73
61	0.98	0.75
62	0.98	0.65
63	0.97	0.73
64	0.96	0.74
65	0.96	0.73
66	0.97	0.72
67	0.97	0.74
68	0.96	0.74
69	0.97	0.72
70	0.98	0.71
71	0.97	0.71
72	0.96	0.70
73	0.97	0.69
74	0.97	0.70
75	0.98	0.75

76	0.97	0.73
77	0.96	0.72
78	0.97	0.74
79	0.97	0.75
80	0.98	0.76
81	0.97	0.70
82	0.96	0.68
83	0.97	0.70
84	0.97	0.68
85	0.98	0.75
86	0.97	0.73
87	0.96	0.73
88	0.96	0.68
89	0.97	0.75
90	0.97	0.73
91	0.98	0.75
92	0.98	0.65
93	0.97	0.73
94	0.96	0.74
95	0.96	0.73
96	0.97	0.72
97	0.97	0.74
98	0.96	0.74
99	0.97	0.72
100	0.98	0.71
101	0.97	0.71
102	0.96	0.70
103	0.97	0.69

104	0.97	0.70
105	0.98	0.75
106	0.97	0.73
107	0.96	0.72
108	0.97	0.74
109	0.97	0.75
110	0.98	0.76
111	0.97	0.70
112	0.96	0.68
113	0.97	0.70
114	0.97	0.68
115	0.98	0.75
116	0.97	0.73
117	0.96	0.73
118	0.96	0.68
119	0.97	0.75
120	0.97	0.73
121	0.96	0.74
122	0.97	0.72
123	0.98	0.71
124	0.97	0.71
125	0.96	0.70
126	0.97	0.69
Total	122.11%	90.75%

Fuente: Formato pre y post test del indicador tiempo medio de la reparación o MTTR

FICHA DE OBSERVACIÓN – RESUMEN DE LOS PRE TEST Y POST TEST

Registro	DIMENSIÓN: Registro		DIMENSIÓN: Diagnóstico		DIMENSIÓN: Resolución	
	PRE TEST	POS TEST	PRE TEST	POS TEST	PRE TEST	POS TEST
1	0.09	0.04	0.15	0.06	101.20%	64.82%
2	0.1	0.04	0.11	0.06	101.00%	74.85%
3	0.06	0.03	0.11	0.05	99.90%	73.29%
4	0.05	0.02	0.12	0.05	99.10%	74.11%
5	0.1	0.05	0.15	0.05	98.95%	72.93%
6	0.1	0.04	0.11	0.04	99.80%	72.22%
7	0.09	0.04	0.16	0.04	99.50%	73.81%
8	0.04	0.04	0.12	0.04	99.16%	73.95%
9	0.07	0.05	0.15	0.04	99.93%	71.95%
10	0.04	0.02	0.15	0.04	100.84%	71.06%
11	0.05	0.03	0.14	0.05	100.48%	71.15%
12	0.08	0.04	0.13	0.04	98.95%	70.19%
13	0.08	0.04	0.13	0.05	100.31%	69.24%
14	0.05	0.03	0.12	0.03	100.41%	69.96%
15	0.06	0.03	0.11	0.03	100.59%	75.11%
16	0.07	0.02	0.1	0.03	100.19%	72.93%
17	0.1	0.03	0.1	0.04	98.95%	72.22%
18	0.05	0.02	0.11	0.03	100.31%	74.18%
19	0.08	0.02	0.13	0.03	100.41%	75.35%
20	0.06	0.02	0.14	0.03	100.59%	75.59%
21	0.06	0.03	0.11	0.04	99.50%	69.55%
22	0.06	0.01	0.16	0.03	99.16%	67.93%
23	0.09	0.02	0.16	0.02	100.31%	69.91%

24	0.05	0.02	0.13	0.02	100.41%	68.37%
25	0.09	0.01	0.13	0.02	100.59%	75.24%
26	0.05	0.01	0.12	0.02	99.50%	72.92%
27	0.06	0.02	0.12	0.03	99.16%	72.53%
28	0.09	0.01	0.11	0.02	98.95%	68.37%
29	0.08	0.01	0.12	0.02	99.80%	75.24%
30	0.07	0.01	0.12	0.02	99.50%	72.91%
31	0.07	0.05	0.11	0.06	101.00%	74.85%
32	0.1	0.04	0.15	0.06	101.20%	64.82%
33	0.06	0.03	0.11	0.05	99.90%	73.29%
34	0.06	0.03	0.12	0.05	99.10%	74.11%
35	0.1	0.05	0.15	0.05	98.95%	72.93%
36	0.1	0.04	0.11	0.04	99.80%	72.22%
37	0.09	0.04	0.16	0.04	99.50%	73.81%
38	0.04	0.04	0.12	0.04	99.16%	73.95%
39	0.09	0.04	0.15	0.04	99.93%	71.95%
40	0.04	0.02	0.15	0.04	100.84%	71.06%
41	0.05	0.03	0.14	0.05	100.48%	71.15%
42	0.08	0.04	0.13	0.04	98.95%	70.19%
43	0.08	0.04	0.13	0.05	100.31%	69.24%
44	0.05	0.03	0.12	0.03	100.41%	69.96%
45	0.05	0.02	0.11	0.03	100.59%	75.11%
46	0.07	0.02	0.1	0.03	100.19%	72.93%
47	0.1	0.03	0.1	0.04	98.95%	72.22%
48	0.05	0.02	0.11	0.03	100.31%	74.18%
49	0.08	0.02	0.13	0.03	100.41%	75.35%
50	0.06	0.02	0.14	0.03	100.59%	75.59%

51	0.06	0.03	0.11	0.04	99.50%	69.55%
52	0.06	0.01	0.16	0.03	99.16%	67.93%
53	0.09	0.02	0.16	0.02	100.31%	69.91%
54	0.05	0.02	0.13	0.02	100.41%	68.37%
55	0.09	0.01	0.13	0.02	100.59%	75.24%
56	0.05	0.01	0.12	0.02	99.50%	72.92%
57	0.06	0.02	0.12	0.03	99.16%	72.53%
58	0.09	0.01	0.11	0.02	98.95%	68.37%
59	0.08	0.01	0.12	0.02	99.80%	75.24%
60	0.07	0.01	0.12	0.02	99.50%	72.91%
61	0.07	0.05	0.11	0.06	101.00%	74.85%
62	0.1	0.04	0.15	0.06	101.20%	64.82%
63	0.06	0.03	0.11	0.05	99.90%	73.29%
64	0.06	0.03	0.12	0.05	99.10%	74.11%
65	0.1	0.05	0.15	0.05	98.95%	72.93%
66	0.1	0.04	0.11	0.04	99.80%	72.22%
67	0.09	0.04	0.16	0.04	99.50%	73.81%
68	0.04	0.04	0.12	0.04	99.16%	73.95%
69	0.09	0.04	0.15	0.04	99.93%	71.95%
70	0.04	0.02	0.15	0.04	100.84%	71.06%
71	0.05	0.03	0.14	0.05	100.48%	71.15%
72	0.08	0.04	0.13	0.04	98.95%	70.19%
73	0.08	0.04	0.13	0.05	100.31%	69.24%
74	0.05	0.03	0.12	0.03	100.41%	69.96%
75	0.05	0.02	0.11	0.03	100.59%	75.11%
76	0.07	0.02	0.1	0.03	100.19%	72.93%
77	0.1	0.03	0.1	0.04	98.95%	72.22%

78	0.05	0.02	0.11	0.03	100.31%	74.18%
79	0.08	0.02	0.13	0.03	100.41%	75.35%
80	0.06	0.02	0.14	0.03	100.59%	75.59%
81	0.06	0.03	0.11	0.04	99.50%	69.55%
82	0.06	0.01	0.16	0.03	99.16%	67.93%
83	0.09	0.02	0.16	0.02	100.31%	69.91%
84	0.05	0.02	0.13	0.02	100.41%	68.37%
85	0.09	0.01	0.13	0.02	100.59%	75.24%
86	0.05	0.01	0.12	0.02	99.50%	72.92%
87	0.06	0.02	0.12	0.03	99.16%	72.53%
88	0.09	0.01	0.11	0.02	98.95%	68.37%
89	0.08	0.01	0.12	0.02	99.80%	75.24%
90	0.07	0.01	0.12	0.02	99.50%	72.91%
91	0.07	0.05	0.11	0.06	101.00%	74.85%
92	0.1	0.04	0.15	0.06	101.20%	64.82%
93	0.06	0.03	0.11	0.05	99.90%	73.29%
94	0.06	0.03	0.12	0.05	99.10%	74.11%
95	0.1	0.05	0.15	0.05	98.95%	72.93%
96	0.1	0.04	0.11	0.04	99.80%	72.22%
97	0.09	0.04	0.16	0.04	99.50%	73.81%
98	0.04	0.04	0.12	0.04	99.16%	73.95%
99	0.09	0.04	0.15	0.04	99.93%	71.95%
100	0.04	0.02	0.15	0.04	100.84%	71.06%
101	0.05	0.03	0.14	0.05	100.48%	71.15%
102	0.08	0.04	0.13	0.04	98.95%	70.19%
103	0.08	0.04	0.13	0.05	100.31%	69.24%
104	0.05	0.03	0.12	0.03	100.41%	69.96%

105	0.06	0.02	0.11	0.03	100.59%	75.11%
106	0.07	0.02	0.1	0.03	100.19%	72.93%
107	0.1	0.03	0.1	0.04	98.95%	72.22%
108	0.05	0.02	0.11	0.03	100.31%	74.18%
109	0.08	0.02	0.13	0.03	100.41%	75.35%
110	0.06	0.02	0.14	0.03	100.59%	75.59%
111	0.06	0.03	0.11	0.04	99.50%	69.55%
112	0.06	0.01	0.16	0.03	99.16%	67.93%
113	0.09	0.02	0.16	0.02	100.31%	69.91%
114	0.05	0.02	0.13	0.02	100.41%	68.37%
115	0.09	0.01	0.13	0.02	100.59%	75.24%
116	0.05	0.01	0.12	0.02	99.50%	72.92%
117	0.07	0.02	0.12	0.03	99.16%	72.53%
118	0.09	0.01	0.11	0.02	98.95%	68.37%
119	0.08	0.01	0.12	0.02	99.80%	75.24%
120	0.09	0.01	0.12	0.02	99.50%	72.91%
121	0.04	0.04	0.15	0.04	99.16%	73.95%
122	0.09	0.04	0.15	0.04	99.93%	71.95%
123	0.06	0.02	0.14	0.05	100.84%	71.06%
124	0.05	0.03	0.13	0.04	100.48%	71.15%
125	0.08	0.04	0.13	0.05	98.95%	70.19%
126	0.08	0.04	0.12	0.03	100.31%	69.24%

Fuente: Resumen de las pruebas pre y post test por dimensión

8.3 Anexo N° 3: Matriz de consistencia

Título del Proyecto de Investigación: Implementación de la auditoría de sistemas en el servicio de atención al usuario en el Ministerio de Educación

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLE	DIMENSIONES	INDICADOR
General	**General**	**General**			
¿Cuál será el efecto de la implementación de la auditoría de sistemas en el servicio de atención al usuario en el Ministerio de Educación?	Determinar el efecto de la implementación de la auditoría de sistemas en el servicio de atención al usuario en el Ministerio de Educación	La implementación de la auditoría de sistemas mejora significativamente el servicio de atención al usuario en el Ministerio de Educación	**INDEPENDIENTE:** Auditoría de Sistemas	****	****
Específicos	**Específicos**	**Específicos**	**VARIABLE**	**DIMENSIONES**	**INDICADOR**
¿Cuál será el efecto de la implementación de la auditoría de sistemas en el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación?	Determinar el efecto de la implementación de la auditoría de sistemas para el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación	La implementación de la auditoría de sistemas reduce el porcentaje de incidentes asignadas incorrectamente en el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación	**DEPENDIENTE:** Servicio de atención al usuario	Registro	Porcentaje de incidentes asignados incorrectamente
¿Cuál será el efecto de la implementación de la auditoría de sistemas en el diagnóstico de incidentes en el servicio de atención al usuario en el	Determinar el efecto de la implementación de la auditoría de sistemas para el diagnóstico de incidentes en el servicio de atención al usuario en el	La implementación de la auditoría de sistemas reduce el porcentaje de incidentes reclamados en el diagnóstico de incidentes en el servicio de		Diagnóstico	Porcentaje de incidentes reclamados

Ministerio de Educación?	Ministerio de Educación	atención al usuario en el Ministerio de Educación			
¿Cuál será el efecto de la implementación de la auditoría de sistemas en la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación?	Determinar el efecto de la implementación de la auditoría de sistemas para la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación	La implementación de la auditoría de sistemas reduce el tiempo medio de resolución en la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación		Resolución	Tiempo medio de reparación o MTTR D=(Tiempo total transcurrido - Tiempo de inactividad / Tiempo total transcurrido)

Fuente: Matriz de consistencia

8.4 Anexo N° 04: Informe de Auditoria para el Servicio de Atención al Usuario del Ministerio de Educación

Inicio de Proyecto: 04 de septiembre de 2018

Fin de Proyecto: 13 de diciembre de 2018

ANTECEDENTES

El Ministerio de Educación presta servicios a nivel nacional para beneficio de aproximadamente 8’728,876 estudiantes[1] y 558,657 docentes[2], los servicios que se brindan son canalizados y atendidos por diversos canales de atención y comunicación: no presencial – Nivel 1 (telefónico, documental, web, correo electrónico, chat) y presencial – Nivel 2.

De acuerdo al **Art. 44** del Reglamento de Organización y Funciones – ROF del MINEDU se establece que la Oficina de Tecnologías de la Información y Comunicación es responsable de conducir el uso de recursos informáticos a su cargo en el sector Educación y proponer políticas, planes, documentos normativos y estándares pertinentes.

Asimismo, de acuerdo **Art. 53** del ROF MINEDU se establece que la Unidad de Servicio de Atención al Usuario es responsable del diseño e implementación de los procesos, procedimientos y métricas para la atención oportuna y asistencia técnica a los usuarios de los servicios informáticos del Ministerio y dependiente de la Oficina de Tecnologías de la Información y Comunicación.

- La sede institucional del MINEDU cuenta con aproximadamente 4,500 usuarios (entre las Sedes principales y desconcentradas) que utilizan los servicios de TI brindados por la OTIC a través del catálogo de servicios de TI publicada en la página web del MINEDU.

- Actualmente, el MINEDU viene atendiendo los incidentes y requerimientos técnicos mediante un servicio de atención de contact center y soporte técnico de servicios de TI, el cual atiende seis (06) centros de atención al ciudadano con provisión de plataformas tecnológicas y recurso humano para atenciones de nivel 1 y 2; así también se cuenta con un centro de atención al ciudadano, para evaluación docente, que cuenta solo con provisión de plataformas tecnológicas.

OBJETIVO GENERAL

Determinar el efecto de la Auditoria de Sistemas para el Servicio de Atención al Usuario en el Ministerio de Educación.

OBJETIVOS ESPECÍFICOS

[1] ***Fuente:*** *Escale 2017*
[2] ***Fuente:*** *Escala 2017*

- Determinar el efecto de la Auditoria de Sistemas para el registro de incidentes en el servicio de atención al usuario en el Ministerio de Educación

- Determinar el efecto de la Auditoria de Sistemas para el diagnóstico de incidentes en el servicio de atención al usuario en el Ministerio de Educación

- Determinar el efecto de la Auditoria de Sistemas para la resolución de incidentes en el servicio de atención al usuario en el Ministerio de Educación.

ALCANCE DE LA AUDITORÍA

Verificar el cumplimiento de ejecución del proceso de Gestión de Incidentes y los procedimientos asociados, los cuales son realizados por la Oficina de Tecnologías de la Información y Comunicación - OTIC.

CONTROL DE LEGALIDAD (CUMPLIMIENTO)

Cumplir con lo establecido en la Norma de Control Interno mediante Resolución de Contraloría N° 320-2006-CG, la misma que es de aplicación a las Entidades del Estado de conformidad con lo establecido por la Ley N° 28716, Ley de Control Interno de la Entidades del Estado.

METODOLOGÍA APLICADA

Se manejó la metodología de MAGERIT para el análisis y gestión de los riesgos, ya que permite determinar los riesgos paso a paso.

A continuación de indican los pasos a seguir:

- **Paso 1:** Inventario de Activos
- **Paso 2:** Amenazas
- **Paso 3:** Salvaguardas

INFORMACIÓN GENERAL DEL SERVICIO DE ATENCIÓN AL USUARIO

La Unidad de Servicio de Atención al Usuario – USAU de la Oficina de Tecnologías de la Información y Comunicación – OTIC viene trabajando la Atención al Usuario bajo las Mejorar Prácticas de la Gestión de Servicios de TI, utilizando el enfoque de ITIL v3. Asimismo, desde el año 2012 ha documentado procesos y procedimientos que cuentan con aprobación, entre ellos tenemos:

Proceso de Gestión de Incidentes: La USAU canaliza las atenciones mediante canales de atención y comunicación, los cuales fueron debidamente socializados con los usuarios de la Entidad, estos canales fueron definidos de la siguiente manera:

Canal telefónico	:	50505
Canal de correo electrónico	:	mesadeayuda@minedu.gob.pe
Web	:	mesadeayuda.minedu.gob.pe

Notificar solicitud: Se recibe la solicitud por los canales de atención y comunicación de TI que son usados en el MINEDU. Quien ejecuta la actividad es el usuario que utiliza los servicios brindados por la OTIC del MINEDU.

Registra solicitud: El agente de atención al usuario, registra la solicitud del usuario mediante el sistema de registro de tickets alimentando una base de datos de atenciones, comprobando que todos los datos estén completos, caso contrario se solicita que complete la información.

Identificar solicitud: El agente de atención al usuario, analiza la solicitud mediante los criterios de solicitud que le han sido proporcionados para determinar su tratamiento de la solicitud.

¿Es incidente?
Sí: Si es un incidente, se procederá a su identificación y clasificación para determinar sí es un error conocido.

No: Si no se trata de un incidente, inmediatamente se activa el subproceso de solicitud, para su atención.

Proceso de solicitud: Al no tratarse de un incidente el agente de atención al usuario activará el proceso de solicitud, donde al finalizar este subproceso, se procederá con el cierre de la solicitud.

Identificar y clasificar incidente: El agente de atención al usuario, clasifica el incidente de acuerdo al catálogo técnico que ha sido alojado en el Intranet de la Entidad, verificando en la base de datos si se trata de un error conocido para su correcta clasificación.
¿Error conocido?
Sí: En caso de ser un error conocido, el agente de atención al usuario identifica las alternativas de solución.
No: En caso de no ser un error conocido, el agente de atención al usuario evalúa la prioridad del incidente.

Evaluar prioridad de incidente: El agente de atención al usuario, deberá consultar a la tabla de prioridades (criterios de prioridad) la misma que estará almacenada en el File Server de la USAU para una correcta evolución.

¿Qué tipo de incidente es?
Incidente grave o de seguridad de la información: Si se trata de un incidente grave o seguridad de información, se activará inmediatamente el subproceso de tratar incidente grave o de seguridad.

Incidente regular: Si se trata de un incidente regular, se procede con la actividad de posibles soluciones.

Tratar incidente graveo de seguridad de la información: El agente de atención al usuario, al no tratarse de un incidente regular activará el subproceso de tratar el incidente

grave o de seguridad de la información donde será escalado para tu tratamiento.

Identificar la posible solución: El agente de atención al usuario, identifica las alternativas de posible solución extraídas de la base de conocimiento de la KB de soluciones para su ejecución.

Identificar alternativas de solución: El agente de atención al usuario, procede a identificar el procedimiento y/o manuales que son necesarios para la resolución de incidentes. La información actual esta almacenada en el File Server de la USAU (KB de procedimientos).

¿Es escalable?
Sí: Si es si, se activa inmediatamente el subproceso de escalamiento de atención a incidentes.
No: Si es no, se ejecuta criterios de solución.

Ejecutar criterios de solución: El agente de atención al usuario, ejecuta las alternativas o posibles soluciones identificadas.

¿Solucionado?
Sí: Si es si, Se notifica la solución al usuario.
No: Si es no, se procede a identificar la posible solución extraídas de la KB de solución.

Sub proceso de escalamiento de atención a incidente: Al reconocer que el incidente es escalable, el agente de atención al usuario, ejecuta el subproceso de escalamiento de atención a incidente para su tratamiento del incidente.

Notificar solución: El agente de atención al usuario, al saber el resultado del subproceso de escalamiento de atención a incidente, procede en notificar la solución del incidente tratado de acuerdo a la condición.

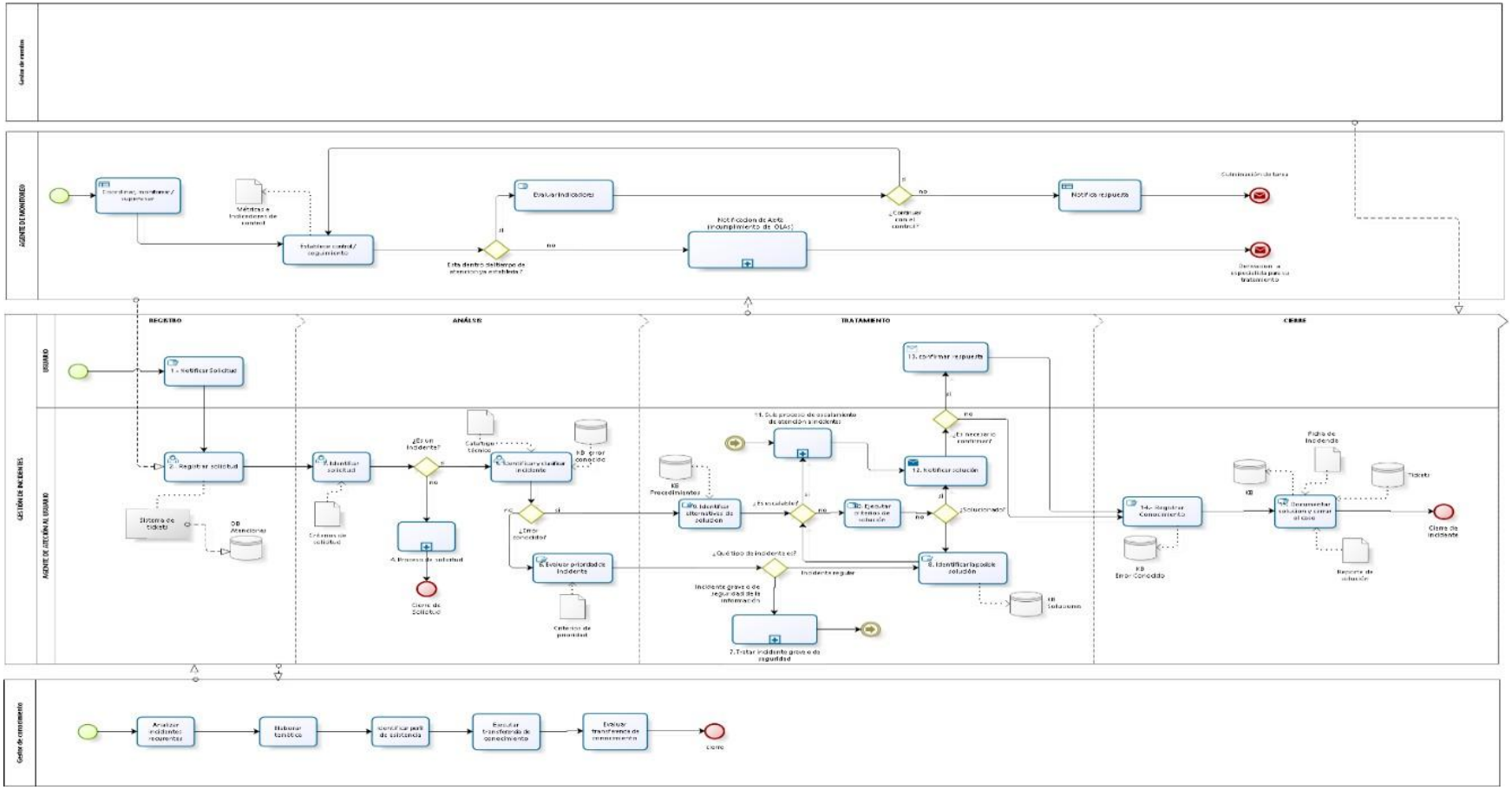
¿Es necesario confirmar?
Sí: Si es necesario, se confirma respuesta del usuario por medio de comunicación.
No: Si no es necesario, se transfiere el conocimiento a la KB de error de conocimiento como registro.

Confirmar respuesta: El usuario, al recibir el correo de confirmación de respuesta, responde a la confirmación de respuesta del incidente para luego ser registrado.

Registrar Conocimiento: El agente de atención al usuario, registra la confirmación de respuesta del usuario si es necesario o solución sin confirmación directa, para su registro a la KB de errores conocidos como parte el proceso de atención al incidente.

Documentar, solucionar y cerrar el caso: El agente de atención al usuario, documenta la solución que le ha sido entregada, ingresando la información a la base de conocimiento, el reporte de solución y ficha de incidente, cerrando al final el proceso de ticket de atención.

Cierre de incidente: Fin del proceso de gestión de Incidentes



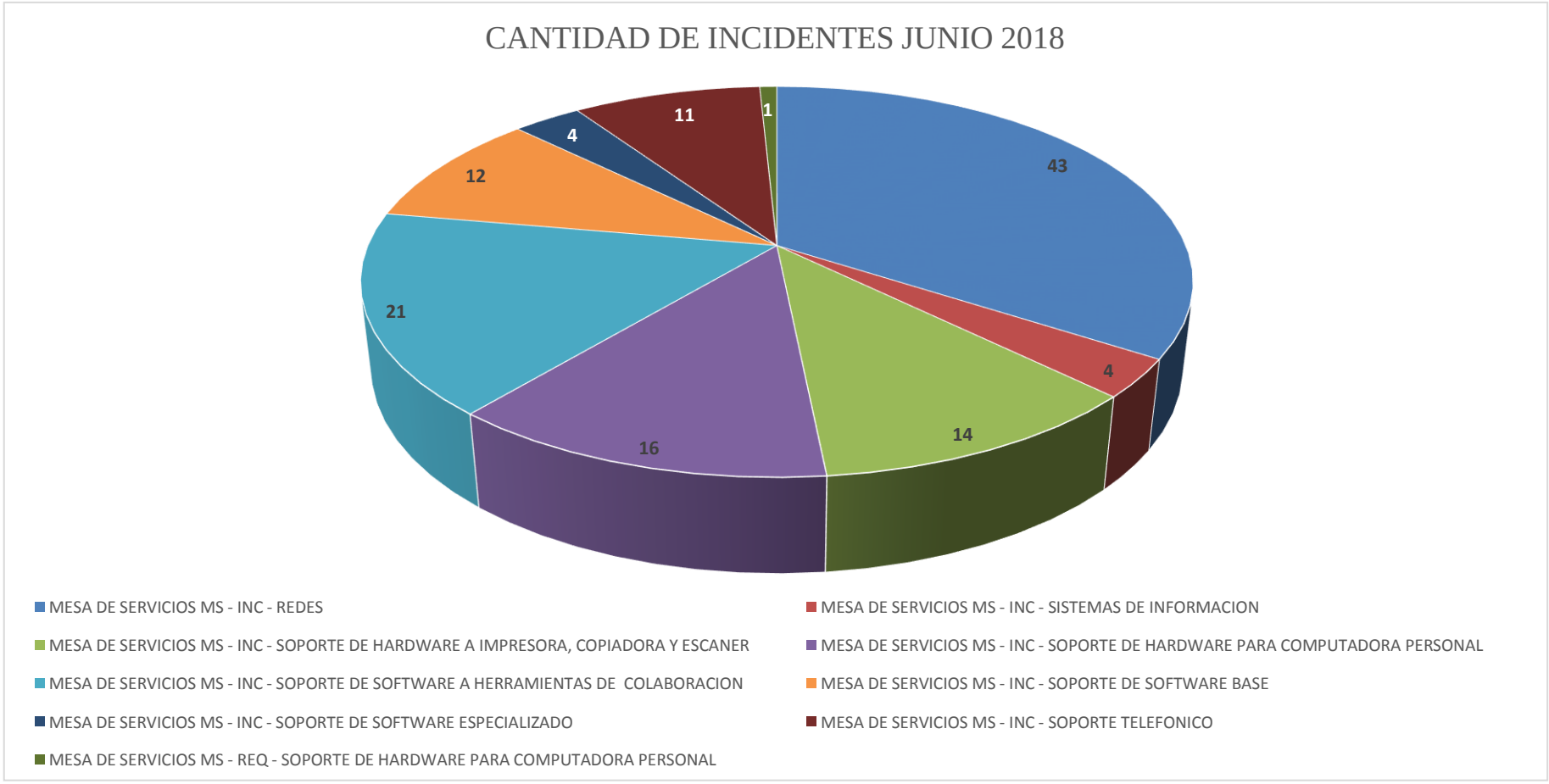
EVALUACIÓN PREVIA A LA AUDITORÍA DE SISTEMAS (Pre Test)

Población = 185 incidentes
Muestra = 126 incidentes
Mes de aplicación: junio 2018

INCIDENTES POR CATEGORÍA - JUNIO 2018

SERVICIO	CATEGORÍA	CANTIDAD DE INCIDENTES JUNIO
MESA DE SERVICIOS	MS - INC - REDES	43
	MS - INC - SISTEMAS DE INFORMACIÓN	4
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	14
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	16
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	21
	MS - INC - SOPORTE DE SOFTWARE BASE	12
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	4
	MS - INC - SOPORTE TELEFÓNICO	11
	MS - REQ - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	1
TOTAL		**126**

Fuente: Incidentes por categoría – junio 2018


CANTIDAD DE INCIDENTES JUNIO 2018
43
4
14
16
21
12
4
11
1
MESA DE SERVICIOS MS - INC - REDES
MESA DE SERVICIOS MS - INC - SISTEMAS DE INFORMACION
MESA DE SERVICIOS MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCANER
MESA DE SERVICIOS MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL
MESA DE SERVICIOS MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACION
MESA DE SERVICIOS MS - INC - SOPORTE DE SOFTWARE BASE
MESA DE SERVICIOS MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO
MESA DE SERVICIOS MS - INC - SOPORTE TELEFONICO
MESA DE SERVICIOS MS - REQ - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL

INCIDENTES POR SUBCATEGORÍA - JUNIO 2018

SERVICIO	CATEGORÍA Y SUBCATEGORÍA	CANTIDAD DE INCIDENTES JUNIO
MESA DE SERVICIOS	**MS - INC - REDES**	**43**
	RED LAN INSTITUCIONAL	41
	VPN	2
	MS - INC - SISTEMAS DE INFORMACIÓN	**4**
	ESCALAFON	1
	PERUEDUCA	1
	SIAF	1
	SIGMA 2.0	1
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**14**
	IMPRESORA INYECCIÓN	1
	IMPRESORA LÁSER	3
	MULTIFUNCIONAL INYECCIÓN	2
	MULTIFUNCIONAL LÁSER	7
	SCANNER	1
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**16**
	DOCKING STATION	1
	LAPTOP	1
	MOUSE	1
	PC	12
	PC AIO	1
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**21**
	ALOJAMIENTO DE ARCHIVOS	1

	CORREO ELECTRÓNICO	17
	INTERNET	3
	MS - INC - SOPORTE DE SOFTWARE BASE	**12**
	ANTIVIRUS	1
	OFIMATICA - OFFICE	10
	SISTEMA OPERATIVO	1
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**4**
	PROGRAMACIÓN	4
	MS - INC - SOPORTE TELEFÓNICO	**11**
	TELEFONO IP	11
	MS - REQ - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**1**
	CPU	1
TOTAL		**126**

Fuente: Incidentes por sub-categorías – junio 2018

INCIDENTES REGISTRADOS INCORRECTAMENTE - JUNIO 2018

SERVICIO	REGISTRO	CATEGORÍA Y SUBCATEGORÍA	CANTIDAD DE INCIDENTES JUNIO
MESA DE SERVICIOS	CORRECTO	**MS - INC - REDES**	**43**
		RED LAN INSTITUCIONAL	41
		VPN	2
		MS - INC - SISTEMAS DE INFORMACIÓN	**4**
		ESCALAFON	1
		PERUEDUCA	1
		SIAF	1
		SIGMA 2.0	1
		MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**14**
		IMPRESORA INYECCIÓN	1
		IMPRESORA LÁSER	3
		MULTIFUNCIONAL INYECCIÓN	2
		MULTIFUNCIONAL LÁSER	7
		SCÁNNER	1
		MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**16**
		DOCKING STATION	1
		LAPTOP	1
		MOUSE	1
		PC	12
		PC AIO	1
		MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**21**
		ALOJAMIENTO DE ARCHIVOS	1
		CORREO ELECTRÓNICO	17

		INTERNET	3
		MS - INC - SOPORTE DE SOFTWARE BASE	**12**
		ANTIVIRUS	1
		OFIMÁTICA - OFFICE	10
		SISTEMA OPERATIVO	1
		MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**4**
		PROGRAMACIÓN	4
		MS - INC - SOPORTE TELEFÓNICO	**11**
		TELEFONO IP	11
	INCORRECTO	**MS - REQ - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL**	**1**
		CPU	1
TOTAL			**126**

Fuente: Incidentes registrados incorrectamente – junio 2018

- En este reporte se evidencia el mal registro por parte del agente de atención de nivel 1, el mismo que categorizó una petición de servicio como incidente, el cual conlleva a un error cuantitativo de incidentes registrado durante el periodo de junio 2018. Asimismo, se identifica que no se aplicó correctamente el procedimiento para la gestión de incidentes perjudicando los acuerdos de niveles de servicio y en consecuencia se genera demora en la atención, debido a que las peticiones de servicio tienen un tiempo holgado de atención, ya que estos son programados y coordinados con el usuario; Además, el nivel de satisfacción del usuario se afecta directamente ante la percepción de demora en la atención.

INCIDENTES MAL DIAGNOSTICADOS - JUNIO 2018

SERVICIO	CATEGORÍA Y SUBCATEGORÍA	DIAGNÓSTICO		CANTIDAD DE INCIDENTES JUNIO
		CORRECTO	INCORRECTO	
MESA DE SERVICIOS	**MS - INC - REDES**	**20**	**23**	**43**
	RED LAN INSTITUCIONAL	20	21	41
	VPN		2	2
	MS - INC - SISTEMAS DE INFORMACIÓN	**1**	**3**	**4**
	ESCALAFON		1	1
	PERUEDUCA		1	1
	SIAF		1	1
	SIGMA 2.0	1		1
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**6**	**8**	**14**
	IMPRESORA INYECCIÓN		1	1
	IMPRESORA LÁSER	2	1	3
	MULTIFUNCIONAL INYECCIÓN		2	2
	MULTIFUNCIONAL LÁSER	4	3	7
	SCÁNNER		1	1
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**11**	**5**	**16**
	DOCKING STATION		1	1
	LAPTOP		1	1
	MOUSE	1		1
	PC	10	2	12
	PC AIO		1	1
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**5**	**16**	**21**

	ALOJAMIENTO DE ARCHIVOS		1	1
	CORREO ELECTRÓNICO	4	13	17
	INTERNET	1	2	3
	MS - INC - SOPORTE DE SOFTWARE BASE	**6**	**6**	**12**
	ANTIVIRUS	1		1
	OFIMATICA - OFFICE	4	6	10
	SISTEMA OPERATIVO	1		1
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**4**		**4**
	PROGRAMACIÓN	4		4
	MS - INC - SOPORTE TELEFÓNICO	**8**	**3**	**11**
	TELEFONO IP	8	3	11
	MS - REQ - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**1**		**1**
	CPU	1		1
TOTAL		**62**	**64**	**126**

Fuente: Incidentes mal diagnosticados – junio 2018

- En este reporte se evidencian los incidentes que tuvieron un tratamiento y no fueron resueltos, debido a un mal diagnóstico del agente de atención de nivel 1, los cuales debieron reabrir los tickets para iniciar nuevamente el procedimiento de incidentes y aplicar, de acuerdo a su expertise o utilizando la KB de incidentes, las posibles alternativas de solución. Las consecuencias de un mal diagnóstico recaen sobre el proceso de atención al usuario (Gestión de Incidentes), ocasionando que los usuarios recurran al canal telefónico para expresar su malestar, en algunos casos recurren ante el Jefe de la OTIC para manifestar su incomodidad y enfado; en estos casos el Jefe de la OTIC se comunica con el Jefe de la USAU para que se tomen las medidas correctivas y se ejecute la atención de manera inmediata, saltando muchas veces los procedimientos establecidos para dicha gestión.

- Se identifica en el reporte que la cantidad de incidentes mal diagnosticados supera a la cantidad de incidentes que fueron registrados correctamente, siendo los porcentajes de correctos 49% y los incorrectos 51%

TIEMPO DE RESOLUCIÓN DE INCIDENTES - JUNIO 2018

SERVICIO	TIEMPO DE RESOLUCIÓN POR CATEGORÍA	CANTIDAD DE INCIDENTES JUNIO
MESA DE SERVICIOS	**MS - INC - REDES**	**43**
	00:00:00	2
	00:01:04	1
	00:02:04	1
	00:03:50	1
	00:06:32	1
	00:09:55	1
	00:27:12	1
	00:27:20	1
	00:30:33	1
	00:34:41	1
	00:35:47	1
	00:45:22	1
	00:46:54	1
	00:59:03	1
	01:11:39	1
	01:15:35	1
	01:17:14	1
	01:21:47	1
	01:33:43	1
	01:37:41	1
	02:00:57	1

	02:09:39	1
	02:13:52	1
	02:20:57	1
	02:21:10	1
	04:36:03	1
	05:09:48	1
	05:46:40	1
	06:31:08	1
	08:17:09	1
	10:46:29	1
	10:47:55	1
	11:04:22	1
	11:04:52	1
	11:32:43	1
	12:01:31	1
	12:51:37	1
	17:11:14	1
	21:48:43	1
	37:28:12	1
	398:50:38	1
	43:32:32	1
	MS - INC - SISTEMAS DE INFORMACIÓN	**4**
	00:00:00	1
	00:17:22	1
	00:30:19	1
	01:01:58	1

	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**14**
	00:46:25	1
	00:48:01	1
	00:49:53	1
	00:57:07	1
	01:06:52	1
	02:42:04	1
	100:28:23	1
	13:25:15	1
	200:40:47	1
	22:28:55	1
	271:40:38	1
	346:39:40	1
	35:57:07	1
	68:57:41	1
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**16**
	00:00:13	1
	00:00:49	1
	00:01:26	1
	00:02:40	1
	00:08:24	1
	01:06:59	1
	02:12:51	1
	03:31:50	1
	03:56:02	1

	07:05:15	1
	08:03:31	1
	10:51:18	1
	11:43:00	1
	14:31:31	1
	311:26:50	1
	32:47:58	1
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**21**
	00:00:00	1
	00:00:41	1
	00:00:52	1
	00:03:39	1
	00:08:18	1
	00:31:17	1
	00:34:55	1
	00:37:03	1
	00:52:46	1
	00:56:07	1
	01:04:40	1
	01:13:04	1
	02:20:43	1
	03:06:31	1
	07:57:32	1
	09:56:43	1
	21:07:59	1
	21:12:24	1

	21:23:56	1
	27:34:00	1
	99:28:19	1
	MS - INC - SOPORTE DE SOFTWARE BASE	**12**
	00:00:00	2
	00:14:17	1
	00:51:24	1
	01:18:30	1
	01:25:55	1
	02:08:13	1
	04:31:51	1
	08:39:17	1
	11:48:51	1
	23:19:54	1
	58:51:43	1
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**4**
	16:20:05	1
	16:59:08	1
	16:59:56	1
	18:55:29	1
	MS - INC - SOPORTE TELEFÓNICO	**11**
	00:00:00	4
	00:01:54	1
	00:20:15	1
	01:55:19	1
	03:11:34	1
	14:52:06	1

	18:12:40	1
	449:01:19	1
	MS - REQ - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**1**
	03:37:32	1
TOTAL		**126**

Fuente: Tiempo de resolución de incidentes – junio 2018

- En este reporte se evidencia que existen tiempos de resolución de incidentes que exceden los acuerdos de niveles de servicio establecidos por la USAU de la OTC, teniendo en consideración que la resolución de incidentes no debe exceder un tiempo máximo de 15´. Sin embargo, las atenciones del periodo comprendido para el mes de junio 2018 tuvieron tiempos de atención en promedio de 8 horas; asimismo, se identificaron incidentes que tuvieron un tiempo de atención de 313 horas en promedio. Como consecuencia de lo identificado, se tuvieron múltiples reclamos de los usuarios, las mismas que fueron canalizadas a través del correo electrónico institucional y llamadas telefónicas a los Jefes de la OTIC y USAU respectivamente.

- Se evidencia, además, que no se cuenta con canales oficiales de atención de quejas, reclamos o sugerencias, las cuales generen una atención personalizada de atenciones que hayan excedido los acuerdos de niveles de servicio o que haya tenido problemas de mala atención por parte de los agentes de atención de nivel 1 o 2.

TIEMPO DE RESOLUCIÓN POR DIAGNÓSTICO - JUNIO 2018

SERVICIO	TIEMPO DE RESOLUCIÓN POR CATEGORÍA	DIAGNÓSTICO		CANTIDAD DE INCIDENTES JUNIO	CANTIDAD DE INCIDENTES DESBORDADOS
		CORRECTO	INCORRECTO		
MESA DE SERVICIOS	**MS - INC - REDES**	**20**	**23**	**43**	**6**
	00:00:00	2		2	
	00:01:04	1		1	
	00:02:04	1		1	
	00:03:50	1		1	
	00:06:32		1	1	
	00:09:55	1		1	
	00:27:12		1	1	
	00:27:20		1	1	
	00:30:33		1	1	
	00:34:41		1	1	
	00:35:47		1	1	
	00:45:22	1		1	
	00:46:54	1		1	
	00:59:03		1	1	
	01:11:39	1		1	
	01:15:35	1		1	
	01:17:14		1	1	
	01:21:47	1		1	
	01:33:43		1	1	
	01:37:41		1	1	
	02:00:57		1	1	

	02:09:39	1		1	
	02:13:52		1	1	
	02:20:57		1	1	
	02:21:10	1		1	
	04:36:03		1	1	
	05:09:48		1	1	
	05:46:40		1	1	
	06:31:08		1	1	
	08:17:09		1	1	
	10:46:29	1		1	
	10:47:55	1		1	
	11:04:22	1		1	
	11:04:52	1		1	
	11:32:43	1		1	
	12:01:31		1	1	
	12:51:37	1		1	
	17:11:14		1	1	
	21:48:43		1	1	
	37:28:12		1	1	
	398:50:38		1	**1**	
	43:32:32	1		1	
	MS - INC - SISTEMAS DE INFORMACIÓN	**1**	**3**	**4**	
	00:00:00	1		1	
	00:17:22		1	1	
	00:30:19		1	1	
	01:01:58		1	1	

	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**6**	**8**	**14**	
	00:46:25		1	1	
	00:48:01	1		1	
	00:49:53	1		1	
	00:57:07	1		1	
	01:06:52		1	1	
	02:42:04	1		1	
	100:28:23		1	**1**	
	13:25:15	1		1	
	200:40:47	1		1	
	22:28:55		1	1	
	271:40:38		1	**1**	
	346:39:40		1	**1**	
	35:57:07		1	1	
	68:57:41		1	1	
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**11**	**5**	**16**	
	00:00:13	1		1	
	00:00:49	1		1	
	00:01:26	1		1	
	00:02:40	1		1	
	00:08:24	1		1	
	01:06:59	1		1	

	02:12:51	1		1	
	03:31:50		1	1	
	03:56:02		1	1	
	07:05:15		1	1	
	08:03:31		1	1	
	10:51:18	1		1	
	11:43:00	1		1	
	14:31:31	1		1	
	311:26:50	1		1	
	32:47:58		1	1	
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**5**	**16**	**21**	
	00:00:00		1	1	
	00:00:41	1		1	
	00:00:52	1		1	
	00:03:39		1	1	
	00:08:18	1		1	
	00:31:17		1	1	
	00:34:55	1		1	
	00:37:03	1		1	
	00:52:46		1	1	
	00:56:07		1	1	
	01:04:40		1	1	
	01:13:04		1	1	
	02:20:43		1	1	

	03:06:31		1	1	
	07:57:32		1	1	
	09:56:43		1	1	
	21:07:59		1	1	
	21:12:24		1	1	
	21:23:56		1	1	
	27:34:00		1	1	
	99:28:19		1	**1**	
	MS - INC - SOPORTE DE SOFTWARE BASE	**6**	**6**	**12**	
	00:00:00	2		2	
	00:14:17	1		1	
	00:51:24	1		1	
	01:18:30		1	1	
	01:25:55	1		1	
	02:08:13		1	1	
	04:31:51		1	1	
	08:39:17		1	1	
	11:48:51		1	1	
	23:19:54		1	1	
	58:51:43	1		1	
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**4**		**4**	
	16:20:05	1		1	
	16:59:08	1		1	
	16:59:56	1		1	

	18:55:29	1		1	
	MS - INC - SOPORTE TELEFÓNICO	**8**	**3**	**11**	
	00:00:00	4		4	
	00:01:54	1		1	
	00:20:15	1		1	
	01:55:19		1	1	
	03:11:34		1	1	
	14:52:06	1		1	
	18:12:40	1		1	
	449:01:19		1	**1**	
	MS - REQ - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**1**		**1**	
	03:37:32	1		1	
TOTAL		**62**	**64**	**126**	

Fuente: Tiempo de resolución por diagnóstico – junio 2018

- Se evidencia que los tiempos extremos de resolución de incidentes se deben directamente a un mal diagnóstico realizado por el agente de atención de nivel 1 o 2. Existen incidentes en menor proporción que cuentan con tiempos extremos de resolución; sin embargo, el mayor porcentaje es por un mal diagnóstico.

ANÁLISIS DE RIESGO (Magerit)

Dentro del presente proceso se identifican los principales activos de TI que son utilizados para brindar el servicio de atención al usuario de manera satisfactoria; asimismo, se identifican los actores que interactúan en el proceso; además se elabora un análisis de riesgo para identificar los riesgos asociados a las atenciones realizadas por la empresa Think IP S.R.L, la metodología utilizada para tal finalidad, fue MAGERIT.

I. Introducción

El presente documento muestra las actividades relacionados a la mejora continua relacionado al Análisis de Riesgos basado en la metodología de MAGERIT, como parte de la Auditoria de Sistemas en el Servicio de Atención al Usuario en el Ministerio de Educación. Para ello, identifica a las partes involucradas, define la interrelación entre actividades, especifica la información de entrada y resultados de salida. Asimismo, se declaran los criterios de control, que conducirán la oportuna acción de los recursos y herramientas en el análisis.

1.1 Objetivo

Suministrar la documentación de la evaluación de riesgos elaborada al Servicio de Atención al Usuario en el Ministerio de Educación. Este orientará el alcance, las actividades y los tiempos, que facilitaran el detalle necesario para comprender el funcionamiento del análisis.

II. Alcance

El presente procedimiento se aplicará para las actividades del equipo de Servicio de Atención al Usuario en el Ministerio de Educación.

III. Marco Normativo

- R.S.G. N° 710-2015 - Directiva 003–2015–MINEDU/SPE-OTIC "Directiva para el Acceso y Uso Adecuado de los Recursos Informáticos en el Ministerio de Educación" y "Directiva para la Administración de los Recursos Informáticos del Ministerio de Educación".
- R.S.G. N°908-2015-MINEDU Directiva N°006-2015-MINEDU/SPE-OPEP-UNOME denominada “Metodología para la gestión por procesos en el Ministerio de Educación”
- R.S.G. N°908-2015-MINEDU Directiva N°007-2015-MINEDU/SPE-OPEP-UNOME denominada “Elaboración, Aprobación y Actualización de los Manuales de Procedimientos (MAPRO) del Ministerio de Educación”
- D.S. N° 109-2012-PCM, aprueba la “Estrategia de Modernización de la Gestión Pública”.
- D.S. N° 004-2013-PCM, “Política Nacional de Modernización de la Gestión Pública”.

IV. Definiciones, siglas y abreviaturas

Se definen los términos empleados en el documento para comprensión del mismo.

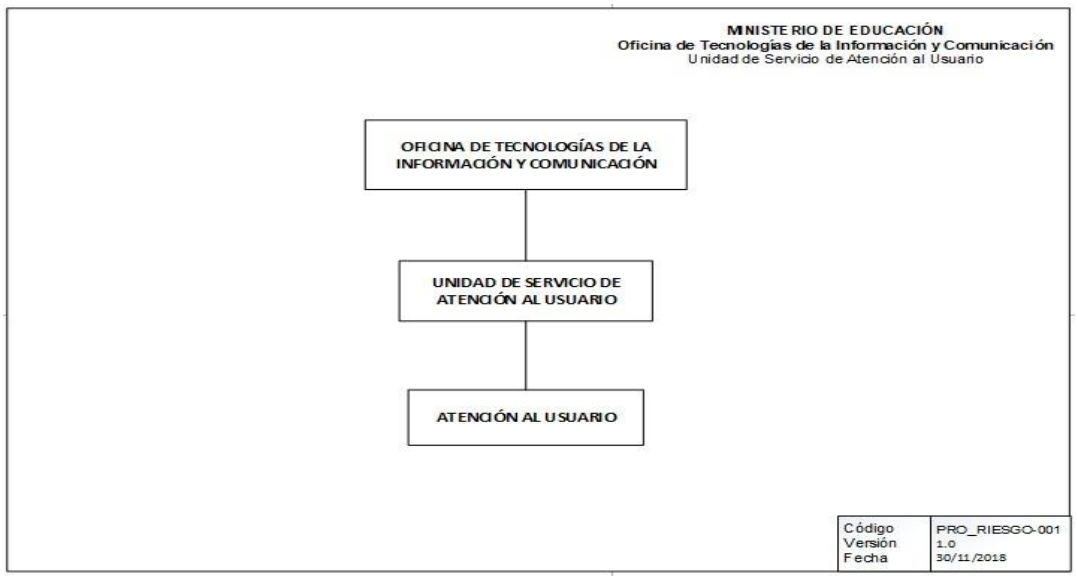
- **MINEDU:** Ministerio de Educación
- **TI:** Tecnologías de la Información
- **OTIC:** Oficina de Tecnologías de la Información y Comunicación
- **USAU:** Unidad de Servicio de Atención al Usuario
- **MAGERIT:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

V. Organización

Para la realización del presente análisis se requiere establecer el organigrama e identificar las partes involucradas que actuaran en la realización de las actividades y tratamiento de la información.

Organigrama

Para la realización del presente análisis se establece el siguiente organigrama funcional.



Fuente: Diagrama de jerarquía en equipo de Atención al Usuario

VI. Partes involucradas

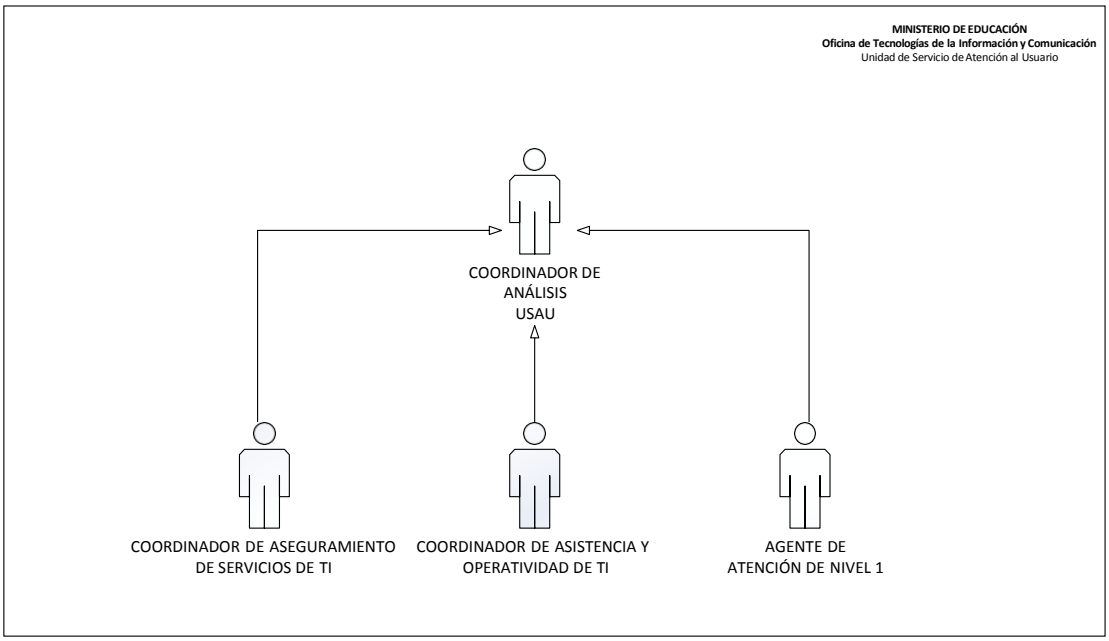
Para la realización del presente análisis se establecen los siguientes roles.

ROL	FUNCIÓN	EQUIPO DE TRABAJO	UNIDAD
Coordinador de Análisis	Responsable de velar por la correcta realización del análisis, medir el rendimiento funcional, y aportar las mejoras al mismo.	Auditor	USAU
Coordinador de Aseguramiento de Servicios de TI	Responsable de velar por la satisfacción de atenciones (incidentes y peticiones) generadas por los usuarios mediante los canales de atención y comunicación de la OTIC.	Aseguramiento de Servicios de TI	USAU
Coordinador de Asistencia y Operatividad de TI	Responsable del cumplimiento de la correcta atención y los acuerdos de nivel de servicio de incidentes y peticiones de los usuarios del Sector Educación, de acuerdo al ámbito de su competencia técnica.	Asistencia y Operatividad de TI	USAU
Agente de atención de Nivel 1	Responsable de atender de manera virtual y clasificar los incidentes solicitados por los usuarios del MINEDU.	Contratista	Think IP

Fuente: Estructura de los roles y responsabilidades

Diagrama de actores

Para la realización del presente procedimiento se establecen los siguientes actores.



Fuente: Estructura orgánica de las partes involucradas

VII. Factores de control para la realización del procedimiento

DESCRIPCIÓN	FUENTE
Documento y/o guía de información necesaria para el análisis de riesgo	Coordinador de Análisis

VIII. Flujos de entrada

- Documentos de atención
- Fichas de Observación

IX. Flujos de salida

- Resultado de Análisis (Hallazgos)

X. Desarrollo de Análisis

Para la realización del presente análisis se requiere establecer los factores necesarios para auditoria de sistemas para el servicio de atención al usuario en el Ministerio de Educación e identificar las partes involucradas que actuarán en la realización de dicha auditoria.

XI. Metodología de evaluación de riesgo

Se manejó la metodología de MAGERIT para el análisis y gestión de los riesgos, ya que permite determinar los riesgos paso a paso.

A continuación de indican los pasos a seguir:

- **Paso 1:** Inventario de Activos de TI
- **Paso 2:** Amenazas identificadas
- **Paso 3:** Salvaguardas

XII. Paso 1: Inventario de Activos

Cada empresa y/o compañía se encargan de proteger la confidencialidad, integridad y disponibilidad de la información para velar la continuidad de sus servicios y mantener su actividad. Con la finalidad de proteger la información de los riesgos y amenazas el Equipo de Atención al Usuario de la Unidad de Servicio de Atención al Usuario - USAU de la Oficina de Tecnologías de la Información – OTIC del Ministerio de

Educación –MINEDU, realizó un inventario de sus activos teniendo en cuenta la Metodología de Magerit los cuales se clasifican en los siguientes grupos:

- Activos esenciales
- Datos o información
- Inventario de servicios
- Las aplicaciones de software.
- Equipos informáticos
- Redes de Comunicación
- Soportes de Información
- Equipamiento Auxiliar
- Instalaciones
- Personal

Datos / Información

Activos esenciales

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área
[Files]	Ficheros	[I_Activos_TI]	Archivo de Inventario de Activos de TI
		[A_Informes y Licencias]	Archivos de Informes y Licencias adquiridas
		[C_Servicio_TI	Contrato de servicio de TI Tercerizados
[backup]	Copia de Respaldo	[A_copias de Seguridad]	Archivos de copias de seguridad de la información (base de datos de tickets y telefonía)
[conf]	Datos de configuración	[D_configuración_comp_srv]	Datos de configuración de computadoras personales y servidores
[int]	Datos de gestión interna	[D_GestiónServicioTI]	Procedimientos de Gestión de Servicios de TI
[password]	Credenciales	[D_credenciales]	Credenciales por usuario

Inventario Servicios

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área
[ext]	A usuarios externos (sedes descentralizadas)	[S_U_Externo]	Servicios prestados a usuarios externos de sede descentralizadas (SIAGIE, PERUEDUCA, SUP, COAR, IIEE)
[int]	Interno (a usuarios propios del MINEDU)	[S_U_Interno]	Servicios prestados a los trabajadores propios del MINEDU (Internet, Correo Electrónico, Gestión de Accesos de TI, Asignación de equipamiento de TI, Mantenimiento de TI, Telefonía)

Software – Aplicaciones informáticas

En vista que la Unidad de Servicio de Atención al Usuario de la OTIC, se dedica a emitir los estados de los activos de TI que mantiene en ejecución los servicios de TI del MINEDU, este cuenta con registros conformado de hojas de cálculo donde se registra, actualiza y almacena las altas, baja de los activos de TI:

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área
[ap]	Aplicaciones	[S_TK_TEL_MO]	Service Desk Plus para el registro y atención de incidentes peticiones
			SIGELLA para atención de llamadas telefónicas
			Nagvis para el monitores de servicios y equipos de comunicación

Equipos informáticos

Se consideran todos los equipos informáticos de la Unidad de Servicio de Atención al Usuario.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[host]	Grandes Equipos (Servidor de base de datos)	[S_Database]	Servidor de Base de Datos (Sistema de tickets y Central Telefónica)
		[S_APL]	Servidor de Aplicaciones (Service Desk y SIGELLA)
[mid]	Equipos Medios (Equipos de trabajo	[PC_agentes]	Computadora personal de Escritorio

	conectados a través de red física)		
[pc]	Equipos que son fáciles de transportar	[PC_portatiles]	Computadora personal portátil
[Cel]	Equipos móviles para comunicación y gestión	[CEL_Agentes]	Equipos móviles para la atención de incidentes y peticiones

Redes de comunicaciones

Se considera todas las redes de comunicación que es usado por la Unidad de Servicio de Atención al Usuario.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[pstn]	Red Telefónica	[R_telefónica]	Red telefónica
[wifi]	Red inalámbrica	[R_wifi]	Red inalámbrica
[mobile]	Telefonía móvil	[T_móvil]	Telefonía móvil
[LAN]	Red local	[R_Local]	Red local
[Internet]	Internet	[Internet]	Internet

Soporte de Información _ almacenamiento electrónico

Se considera dispositivos físicos de almacenamiento electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[san]	Almacenamiento en servidor	[A_BD]	Base de datos del sistema de tickets y central telefónica
[cd]	Discos	[A_HDD]	Almacenamientos en Disco Duro Externo

Soporte de Información _ almacenamiento no electrónico

Se considera dispositivos físicos de almacenamiento electrónico.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[printed]	Material impreso	C_ Documentación_Activos_TI	Carpetas con la documentación de cada alta y baja (ctm, orden, propuestas de postor, orden compra guía de remisión evaluación técnica)
		C_Reporteseinformes	Carpetas de reporte e informes impresos de atenciones por garantía.
		C_fichasdemovimientos	Carpetas con ficha de movimientos de los activo informáticos

Equipamiento Auxiliar

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[printed]	Sistema de alimentación interrumpida	U_Servidores	UPS para servidores
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales (papel, sobres, carpetas, etc.)
[Fumiture]	Mobiliario	M_Mobiliario	Mobiliario (Módulos, escritorios, archivadores, armarios, etc.)

Instalaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[building]	Edificio	E_empresa	Instalación de la Sede Centromin y Sede Central y Contratista

Personal

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa
[ui]	Usuarios internos	C_CASTI	Coordinador de Aseguramiento de Servicios de TI
		A_CAOTI	Coordinador de Asistencia y Operatividad de TI
		Ag_N1_N2	Agente de Atención de Nivel 1 y 2

Valoración cualitativa de los activos

Sabiendo que todos los activos no tienen la misma importancia para una empresa y en el caso de que sean atacados o presente una incidencia generará un impacto diferente en la institución, por tal se realiza una valorización cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad como es la confidencialidad, integridad y disponibilidad según a la siguiente tabla.

Tabla N°01: Criterios de Valoración

VALOR		CRITERIO
10	Extremo	Daño extremadamente grande
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	despreciable	Irrelevante a efectos prácticos

Fuente: Tomado del MAGERIT v3 libro 2 Catalogo de elementos

Valoración Cualitativa de Activos esenciales

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de seguridad de la información	Criterio
[vr]	Datos vitales	[I_Activos_TI]	Información de Activos de TI (base de datos, aplicaciones y equipamiento)	Confidencialidad	8
				Integridad	7
				Disponibilidad	7
		[I_Licencias]	Información de Licencias	Confidencialidad	3
				Integridad	7
				Disponibilidad	7
[classified]	Datos clasificados	[E_S_Licenciado]	Ejecutable software Licenciado	Confidencialidad	5
				Integridad	7
				Disponibilidad	7
		[D_Historicos]	Información Histórica de activos de TI	Confidencialidad	5
				Integridad	5
				Disponibilidad	5

Valoración Cualitativa Datos / Información

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de seguridad de la información	Criterio
[Files]	Ficheros	[I_Activos_TI]	Archivo de Inventario de Activos de TI	Confidencialidad	8
				Integridad	5
				Disponibilidad	7
		[A_Informes y Licencias]	Archivos de Informes y Licencias adquiridas	Confidencialidad	8
				Integridad	5
				Disponibilidad	7
		[C_Servicio_TI	Contrato de servicio de TI tercerizados	Confidencialidad	2
				Integridad	6
				Disponibilidad	6
[backup]	Copia de Respaldo	[A_copias de Seguridad]	Archivos de copias de seguridad de la información (base de datos de tickets y telefonía)	Confidencialidad	7
				Integridad	6
				Disponibilidad	6
[conf]	Datos de configuración	[D_configuración_comp_srv]	Datos de configuración de computadoras personales y servidores	Confidencialidad	8
				Integridad	8
				Disponibilidad	6
[int]	Datos de gestión interna	[D_GestiónServicioTI]	Procedimientos de Gestión de Servicios de TI	Confidencialidad	3
				Integridad	3
				Disponibilidad	3
[password]	Credenciales	[D_credenciales]	Credenciales por usuario	Confidencialidad	8
				Integridad	6
				Disponibilidad	6

Valoración Cualitativa Servicios

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de seguridad de la información	Criterio
[ext]	A usuarios externos (sedes descentralizadas)	[S_U_Externo]	Servicios prestados a usuarios externos de sede descentralizadas (SIAGIE, PERUEDUCA, SUP, COAR, IIEE)	Confidencialidad	3
				Integridad	3
				Disponibilidad	7
[int]	Interno (a usuarios propios del MINEDU)	[S_U_Interno]	Servicios prestados a los trabajadores propios del MINEDU (Internet, Correo Electrónico, Gestión de Accesos de TI, Asignación de equipamiento de TI, Mantenimiento de TI, Telefonía)	Confidencialidad	3
				Integridad	3
				Disponibilidad	7

Valoración Cualitativa Software – Aplicaciones informáticas

En vista que la Unidad de Servicio de Atención al Usuario de la OTIC, se dedica a emitir los estados de los activos de ti que mantiene en ejecución los servicios de TI del MINEDU, este cuenta con registros conformado de hojas de cálculo donde se registra, actualiza y almacena las altas, baja de los activos de TI.

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Dimensión de seguridad de la información	Criterio
[ap]	Aplicaciones	[S_TK_TEL_MO]	Service Desk Plus para el registro y	Confidencialidad	3

			atención de incidentes peticiones	Integridad	7
				Disponibilidad	7
			SIGELLA para atención de llamadas telefónicas	Confidencialidad	3
				Integridad	5
				Disponibilidad	7
			Nagvis para el monitoreo de servicios y equipos de comunicación	Confidencialidad	6
				Integridad	6
				Disponibilidad	8

Valoración Cualitativa de Equipos informáticos

Se consideran todos los equipos informáticos de la Unidad de Servicio de Atención al Usuario.

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de seguridad de la información	Criterio
[host]	Grandes Equipos (Servidor de base de datos)	[S_Database]	Servidor de Base de Datos (Sistema de tickets y Central Telefónica)	Confidencialidad	8
				Integridad	8
				Disponibilidad	8
		[S_APL]	Servidor de Aplicaciones (Service Desk y SIGELLA)	Confidencialidad	8
				Integridad	8
				Disponibilidad	8
[mid]	Equipos Medios (Equipos de trabajo conectados a través de red física)	[PC_agentes]	Computadora personal de Escritorio	Confidencialidad	5
				Integridad	5
				Disponibilidad	7
[pc]	Equipos que son fáciles de transportar	[PC_portatiles]	Computadora personal portátil	Confidencialidad	5
				Integridad	5
				Disponibilidad	7

[Cel]	Equipos móviles para comunicación y gestión	[CEL_Agentes]	Equipos móviles para la atención de incidentes y peticiones	Confidencialidad	3
				Integridad	3
				Disponibilidad	5

Valoración cualitativa de redes de comunicaciones

Se considera todas las redes de comunicación que es usado por la Unidad de Servicio de Atención al Usuario:

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de seguridad de la información	Criterio
[pstn]	Red Telefónica	[R_telefónica]	Red telefónica	Confidencialidad	3
				Integridad	3
				Disponibilidad	7
[wifi]	Red inalámbrica	[R_wifi]	Red inalámbrica	Confidencialidad	3
				Integridad	3
				Disponibilidad	7
[mobile]	Telefonía móvil	[T_móvil]	Telefonía móvil	Confidencialidad	3
				Integridad	3
				Disponibilidad	5
[LAN]	Red local	[R_Local]	Red local	Confidencialidad	5
				Integridad	3
				Disponibilidad	7
[Internet]	Internet	[Internet]	Internet	Confidencialidad	3
				Integridad	3
				Disponibilidad	6

Valoración Cualitativas de Soporte de Información _ almacenamiento electrónico

Se considera dispositivos físicos de almacenamiento electrónico:

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de seguridad de la información	Criterio
[san]	Almacenamiento en servidor	[A_BD]	Base de datos del sistema de tickets y central telefónica	Confidencialidad	5
				Integridad	8
				Disponibilidad	8
[cd]	Discos	[A_HDD]	Almacenamientos en Disco Duro Externo	Confidencialidad	6
				Integridad	6
				Disponibilidad	8

Valoración Cualitativa de Soporte de Información _ almacenamiento no electrónico

Se considera dispositivos físicos de almacenamiento no electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de seguridad de la información	Criterio
[printed]	Material impreso	C_ Documentación _Activos_TI	Carpetas con documentación de cada alta y baja (CTM, orden, propuestas de postor, orden compra guía de remisión evaluación técnica)	Confidencialidad	3
				Integridad	6
				Disponibilidad	6
		C_Reporteseinformes	Carpetas de reporte e informes impresos de atenciones por garantía.	Confidencialidad	3
				Integridad	3
				Disponibilidad	3
		C_fichasdemovimientos	Carpetas con ficha de movimientos de los activo informáticos	Confidencialidad	3
				Integridad	3
				Disponibilidad	3

Valoración Cualitativa de Equipamiento Auxiliar

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de seguridad de la información	Criterio
[printed]	Sistema de alimentación interrumpida	U_Servidores	UPS para servidores	Confidencialidad	1
				Integridad	2
				Disponibilidad	6
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales	Confidencialidad	1

			(papel, sobres, carpetas, etc.)	Integridad	1
				Disponibilidad	1
[Fumiture]	Mobiliario	M_Mobiliario	Mobiliario (Módulos, escritorios, archivadores, armarios, etc.)	Confidencialidad	1
				Integridad	1
				Disponibilidad	3

Valoración Cualitativa de Instalaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de seguridad de la información	Criterio
[building]	Edificio	E_empresa	Instalación de la Sede Centromin, Central y Contratista	Confidencialidad	6
				Integridad	6
				Disponibilidad	7

Valoración Cualitativa de Personal

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión de seguridad de la información	Criterio
[ui]	Usuarios internos	C_CASTI	Coordinador de Aseguramiento de Servicios de TI	Confidencialidad	7
				Integridad	10
				Disponibilidad	7
		A_CAOTI	Coordinador de Asistencia y Operatividad de TI	Confidencialidad	7
				Integridad	10
				Disponibilidad	7
		Ag_N1_N2	Agente de Atención de Nivel 1 y 2	Confidencialidad	7
				Integridad	7
				Disponibilidad	7

XIII. Paso 2: Identificación de Amenazas

La probabilidad de las amenazas se realiza teniendo en cuenta la frecuencia con la que

pueda ocurrir, además para las dimensiones de atención al usuario se toma de acuerdo

a esta investigación a si se tomara la escala de rango porcentual de impactos en los activos.

Escala de rango de Probabilidad de amenaza

En el siguiente cuadro se determina los rangos y valores de probabilidad de amenaza en la Unidad de Servicio de Atención al Usuario de la OTIC.

VULNERABILIDAD	RANGO	VALOR
Casi Seguro	1 vez al día	100
Muy probable	1 vez cada semana	70
Probable	1 vez cada 2 meses	50
Poco probable	1 vez al 6 meses	10
Improbable	1 vez al año	5

Fuente: Modulo de Seguridad de la Información

Dimensión de Seguridad MAGERIT

DIMENSIONES A VALORAR	IDENTIFICACIÓN
Confidencialidad	C
Integridad	I
Disponibilidad	D

Fuente: MAGERIT 3.0

Escala de rango porcentual de impactos en los activos para cada dimensión

En el siguiente cuadro se determina la escala porcentual de impacto en los activos en la Unidad de Servicio de Atención al Usuario de la OTIC:

IMPACTO	VALOR CUALITATIVO
Extremo	**100%**
Alto	**75%**
Medio	**50%**
Bajo	**20%**
Mínimo	**5%**

Fuente*:* Modulo de Seguridad de la Información

Escala del impacto y la probabilidad de las amenazas

En base a las tablas predecesoras donde se detalla la escala del impacto y la probabilidad de las amenazas, se procede a identificar las amenazas para el inventario de activos realizado.

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión (%)**		
			[C]	**[I]**	**[D]**
[N.1] Fuego [N.2] Daños por agua	Equipos informáticos	10			100 %
	Instalaciones	10			100 %
[I.1] Fuego [I.2] Daños por agua	-Equipos informáticos -Instalaciones	10			100%
N.1] Fuego [N.2] Daños por agua	Soporte de almacenamiento electrónico y no electrónico	10			100 %
[I.1] Fuego [I.2] Daños por agua	Soporte de almacenamiento electrónico y no electrónico	10			100 %
[N.1] Fuego [N.2] Daños por agua	Equipamiento Auxiliar	5			50 %
[I.1] Fuego [I.2] Daños por agua	Equipamiento Auxiliar	5			50 %
[N.*] Desastres industriales	Equipos informáticos	10			100 %
	Soporte de Información	5			75 %
	Equipamiento Auxiliar	5			20 %
	Instalaciones	5			100%
[I.*] Desastres industriales	Equipos informáticos	10			100 %
	Soporte de Información	5			75 %
	Equipamiento Auxiliar	5			20 %
	Instalaciones	5			100%
[I.3] Contaminación mecánica	Equipos informáticos	50			75%
	Soporte de Información	5			50%
	Equipamiento Auxiliar	5			20%
[I.5] Avería de origen físico o lógico	Software - Aplicaciones Informáticas	50			100%
	Equipos informáticos	10			100%
	Soportes de Información	5			20%
	Equipamiento Auxiliar	5			20%
[I.6] Corte del suministro eléctrico	Equipos Informáticos	50			100%
	Soporte de Información (electrónicos)	5			50%
	UPS	5			5%
[I.7] Condiciones inadecuadas de temperatura o	Equipos Informáticos	50			100%

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión (%)**		
			[C]	**[I]**	**[D]**
humedad					
[I.8] Fallo de servicios de comunicaciones	Redes de comunicaciones (Red inalámbrica, red local e internet)	50			100%
[I.9] Interrupción de otros servicios y suministros esenciales.	Equipamiento Auxiliar	5			5 %
[I.10] Degradación de los soportes de almacenamiento de la información.	Soportes de Información	5			5%
[E.1] Errores de los usuarios **Datos /Información**	Archivos de Informes y Licencias adquiridas	10	100%	100 %	50 %
	Archivos de copias de seguridad de la información	5	100%	100 %	50 %
	Datos de configuración de servidores	5	100%	100 %	50 %
	Datos de Gestión de Activos	5	100%	100%	100%
	Credenciales por usuario	5	50 %	50 %	50 %
	Datos de validación de credenciales por usuarios	5	50 %	50 %	50 %
[E.1] Errores de los usuarios **Servicios**	Servicios prestados a los trabajadores propios del MINEDU	5	100%	100%	75%
	Servicios de Telefonía móvil institucional	10	75 %	50 %	50 %
	Gestión de privilegios de acuerdo al rol dentro de la institución y el lugar de donde esté ingresando, considerando el desempeño.	5	50 %	50 %	75 %
	Soportes de Información almacenamiento electrónico.	10	50 %	50 %	50 %
[E.1] Errores de los usuarios. **Soporte de información**	Soportes de Información _almacenamiento no electrónico.	10	50 %	50 %	50 %
	Datos/Información	50	100 %	75%	50%
[E.2] Errores del administrador	Servicios	5	75%	50%	75%
	Aplicaciones	5	100%	75%	75%
	Redes de Comunicación	10	100%	75%	75%
	Datos de configuración de servidores y equipos	5		100%	
[E.4] Errores de configuración.	Coordinador de Configuración y activos	50		75%	

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión (%)**		
			[C]	**[I]**	**[D]**
[E.7] Deficiencias en la organización	Analista de Configuración y Activos	50		75%	
	Agente de configuración y Activos	50		75%	
	Software –Aplicaciones Informáticas	5	50%	50%	75%
[E.8] Difusión de software dañino	Servicios	5		20%	
[E.9] Errores de [re-]encaminamiento	Software-aplicaciones Informáticas	5		20%	
	Redes de comunicaciones	5		20%	
	Activos esenciales	5		100%	
[E.14] Escapes de información	Datos / información	5		100%	
	Datos / información	10			100%
[E.15] Alteración accidental de la información	Datos / información	10			
[E.18] Destrucción de información	Aplicaciones	5			50%
	Soporte Información	5			20%
	Datos / información	10	75%		
[E19] Fuga de información	Servicios	10	75%		
	Aplicaciones	10	50%		
	Personal	10	75%		
	Office 2013	10	50%	20%	75%
[E20] Vulnerabilidades de los programas	Service Desk Plus para el registro y atención de incidentes peticiones	10	50%	20%	75%
	SIGELLA para atención de llamadas telefónicas	5	75%	20%	100%
	NAVGIS				
	Service Desk Plus para el registro y atención de incidentes peticiones	5		20%	20%
[E21] Errores de mantenimiento/actualización de programas (software)	SIGELLA para atención de llamadas telefónicas	10		50%	50%
	NAVGIS	10		5%	20%
	Servicios	5			100%
[E.24] Caída del sistema por agotamiento de recursos	Equipos informáticos	10			100%
	Redes de comunicaciones	5			100%
	Equipos informáticos	5	75%		100%
[E.25] Pérdida de equipos - Robo	Soporte informático	5	20%		100%
	Equipamiento auxiliar	5	5%		20%
	Datos / información	5	75%		75%
[A.5] Suplantación de la identidad del usuario	Servicios	5	75%		50%
	Aplicaciones	5	75%		50%
	Redes de Comunicaciones	5	75%		75%

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión (%)**		
			[C]	**[I]**	**[D]**
	Datos / información	5	75%	100%	5%
[A.6] Abuso de privilegios de acceso	Servicios	5	50%	50%	75%
	Equipos informáticos	50	75%	75%	75%
	Redes de Comunicaciones	10	75%	50%	75%
	Servicios	5	75%	75%	75%
[A.7] Uso no previsto	Aplicaciones	10	75%	75%	75%
	Equipos Informáticos	50	75%	75%	75%
	Redes de comunicaciones	10	75%	75%	75%
	Soporte de información	5	20%	20%	20%
	Equipamiento Auxiliar	5	20%	20%	20%
	Instalaciones	10	75%	50%	20%
	Aplicaciones	5	50%	75%	75%
[A.8]Difusión de software dañino	Datos / información	10	100%	75%	50%
[A.11] Acceso no autorizado	Servicios	5	75%	50%	50%
	Aplicaciones	10	75%	50%	50%
	Equipos informáticos	10	75%	20 %	75%
	Redes de Comunicaciones	10	75%	20%	75%
	Soporte de información	5	20%	20%	20%
	Equipamiento Auxiliar	5	5%	5%	5%
	Instalaciones	5	75%	20%	20%
	Servicios	5		50%	
A.13] Repudio	Redes de comunicaciones	5	75%		
[A.14] Interceptación de información (escucha pasiva)	Datos / información	5		75%	
A.15] Modificación deliberada de la información	Servicios	5		75%	
	Aplicaciones	5		75%	
	Datos / información	5			100%
[A.18] Destrucción de información	Servicios	5			100%
	Aplicaciones	5			100%
	Soporte de la información	5			75%
	Datos / información	10	100%		
[A.19] Divulgación de información	Soporte de la información	5			
	Aplicaciones	10	100%	100%	100%
[A.22] Manipulación de programas	Equipos informáticos	50	75%		100%
[A.23] Manipulación de los equipos	Soporte de la información	5	20%		20%
	Equipamiento Auxiliar	5	5%		5%
	Equipos informáticos	5			75%
[A.24] Denegación de servicio	Servicios	5			75%
	Redes de comunicaciones	5			75%
	Equipos informáticos	5	75%		100%
[A.25] Robo	Equipamiento Auxiliar	5	75%		20%
	Soporte de la información	5	75%		20%
[A.26] Ataque destructivo	Equipos informáticos	5			100%
	Equipamiento Auxiliar	5			50%

RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU PROBABILIDAD E IMPACTO					
Amenaza	**Activo**	**Probabilidad de Amenaza**	**Impacto para cada Dimensión (%)**		
			[C]	**[I]**	**[D]**
	Instalaciones	5			50%
	Personal	5			75%
A.28] Indisponibilidad del Personal	Personal	5	75%	75%	75%
[A.29] Extorsión	Personal	5	75%	75%	75%
[A.30] Ingeniería Social					

XIV. Paso 3: Salvaguardas

Una vez culminado el inventario de activos y haber identificado las amenazas y vulnerabilidades, se definirán las salvaguardas que son procedimientos tecnológicos que reduce el riesgo, de acuerdo a los activos que se van proteger, para esta investigación se tendrá en cuenta las salvaguardas definidas en MAGERIT.

Tipos de Salvaguardas

Para clasificar los tipos de salvaguardas, se basó en lo indicado en la metodología MAGERIT, tal como se detalla en la siguiente tabla.

EFECTO	TIPO
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Salvaguardas de Activos esenciales

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[vr]	Datos vitales	[I_Activos_TI]	Información de Activos de TI (base de datos y registro de altas y bajas)	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Recuperación (RC)	Respaldo de

					Seguridad – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado.
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
		[I_Licencias]	Información de Licencias	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
[classified]	Datos clasificados	[I_S_Licenciado]	Instalador software Licenciado	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno

					por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
		[D_Historicos]	Información Histórica de activos de TI	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Recuperación (RC)	Respaldo de Seguridad – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.

Salvaguardas de Datos / Información

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[Files]	Ficheros	[I_Activos_TI]	Archivo de Activos de TI	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de

					calidad.
				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
		[A_Informes y Licencias]	Archivos de Informes y Licencias adquiridas	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
[backup]	Copia de Respaldo	[A_copias de Seguridad]	Archivos de copias de seguridad de la información	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.

				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
[conf]	Datos de configuración	[D_configuración_PC]	Datos de configuración de computadoras personales	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Recuperación (RC)	Respaldo de Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
[int]	Datos de gestión interna	[D_GestiónActivos]	Datos de Gestión de Activos	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Recuperación (RC)	Respaldo de

					Seguridad de los archivos de licencias – uno por semana
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.
[password]	Credenciales	[D_credenciales]	Credenciales por usuario	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.

Salvaguardas de Servicios

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).

[int]	Interno (a usuarios propios del MINEDU)	[S_U_Interno]	Servicios prestados a los trabajadores propios del MINEDU	Preventivas (PR)	APO01.08 Mantener el cumplimiento con las políticas y procedimientos.
				Concienciación (AW)	APO.07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
[int]	Interno (a usuarios propios del MINEDU)	[S_Telefonia_Movil]	Servicios de telefonía móvil prestado a los trabajadores propios del MINUEDU	Preventivas (PR)	APO01.08 Mantener el cumplimiento con las políticas y procedimientos.
				Concienciación (AW)	APO.07.06 Mantener las habilidades y competencias del personal.
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
[ipm]	Gestión de privilegios	[G_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la institución y el lugar de donde esté ingresando, considerando el desempeño.	Preventivas (PR)	APO07.01 Mantener la dotación de personal suficiente y adecuado.
				Concienciación (AW)	APO.07.06 Mantener las habilidades y competencias del personal.
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
				Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.

Salvaguardas de Software – Aplicaciones informáticas

Código grupos de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo al Área	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[ap]	Aplicaciones	[S_TK_TEL_MO]	Service Desk Plus para el registro y atención de incidentes peticiones	Preventivas (PR)	APO01.02 Establecer roles y responsabilidades.
			SIGELLA para atención de llamadas telefónicas	Concienciación (AW)	APO.07.06 Mantener las habilidades y competencias del personal.
			NAGVIS	Eliminatorias (EL)	APO01.06 Definir la propiedad de la información (datos) y del sistema.

Salvaguardas de Equipos informáticos

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo al Área	Tipo de Protección	Des. Salvaguarda
[host]	Grandes Equipos (Servidor de base de datos)	[S_Database]	Servidor de Base de Datos	Preventivas (PR)	APO01.02 Establecer roles y responsabilidades.
				Correctivas(CR)	DSSO2.02 Registrar, clasificar y priorizar los registros de incidencias
				Minimización (IM)	DSSO2.05 Resolver y recuperarse ante incidentes
				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Monitorización (Mn)	EDM03.01 Evaluar la gestión de riesgos
				Eliminatorias (EL)	DDS02.05 Resolver y recuperarse ante incidentes

Salvaguardias de Redes de comunicaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo al área	Tipo de Protección	Des. Salvaguarda
[pstn]	Red Telefónica	[R_telefónica]	Red telefónica	Preventivas (PR)	APO01.02 Establecer roles y responsabilidades.
				Correctivas(CR)	DSSO2.02 Registrar, clasificar y priorizar los registros de incidencias
				Minimización (IM)	DSSO2.05 Resolver y recuperarse ante incidentes

[wifi]	Red inalámbrica	[R_wifi]	Red inalámbrica	Preventivas (PR)	APO01.02 Establecer roles y responsabilidades.
				Correctivas(CR)	DSSO2.02 Registrar, clasificar y priorizar los registros de incidencias
				Minimización (IM)	DSSO2.05 Resolver y recuperarse ante incidentes
[LAN]	Red local	[R_Local]	Red local	Preventivas (PR)	APO01.02 Establecer roles y responsabilidades.
				Correctivas(CR)	DSSO2.02 Registrar, clasificar y priorizar los registros de incidencias
				Minimización (IM)	DSSO2.05 Resolver y recuperarse ante incidentes
[Internet]	Internet	[Internet]	Internet	Preventivas (PR)	APO01.02 Establecer roles y responsabilidades.
				Correctivas(CR)	DSSO2.02 Registrar, clasificar y priorizar los registros de incidencias
				Minimización (IM)	DSSO2.05 Resolver y recuperarse ante incidentes

Salvaguardas de Soporte de Información _ almacenamiento electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[san]	Almacenamiento en Red	[A_UR]	Almacenamiento en Red	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Concienciación (AW)	APO07.01 Mantener la dotación de

					personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
[cd]	Discos	[A_CD]	Almacenamientos en Disco Duro	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).

Salvaguardas de Soporte de Información _ almacenamiento no electrónico

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[printed]	Material impreso	C_ Documentación_ Activos_TI	Carpetas con la documentación de cada alta y baja (ctm, orden, propuestas de postor, orden compra guía de remisión evaluación técnica)	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
		C_Reporteseinformes	Carpetas de reporte e informes impresos de atenciones por garantía.	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.

				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
		C_fichasdemovimientos	Carpetas con ficha de movimientos de los activo informáticos	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).

Salvaguardas de Equipamiento Auxiliar

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[printed]	Sistema de alimentación interrumpida	U_Computadores	UPS computadora personal de escritorio	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
[suplly]	Suministros Esenciales	Esenciales	Suministros esenciales (papel,	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares,

			sobres, carpetas, etc.)		procesos y prácticas de calidad.
				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
[Fumiture]	Mobiliario	M_Mobiliario	Mobiliario (Módulos, escritorios, archivadores, armarios, etc.)	Preventivas (PR)	APO.11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.
				Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).

Salvaguardias de Instalaciones

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[building]	Edificio	E_empresa	Instalación de la Sede Centromin	Disuasión (DR)	MEA01.01 Establecer un esquema de supervisión
				Detección(DC)	MEA01.04 Analizar e informar sobre el rendimiento

Salvaguardas Cualitativa de Personal

Código grupo de activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des. Salvaguarda
[ui]	Usuarios internos	C_CASTI	Coordinador de Aseguramiento de Servicios de TI	Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
		A_COATI	Coordinador de Asistencia y Operatividad de TI	Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).
		Ag_N1	Agente de Atención de Nivel 1	Concienciación (AW)	APO07.01 Mantener la dotación de personal suficiente y adecuado
				Administrativas (AD)	APO11.01 Establecer un sistema de gestión de la calidad (SGC).

XV. Métricas

- Número de Riesgos a los sistemas de información.
- Número de Salvaguardas para los activos de TI.
- Número de Amenazas a los sistemas de información.
- Número de conformidades de accesos.

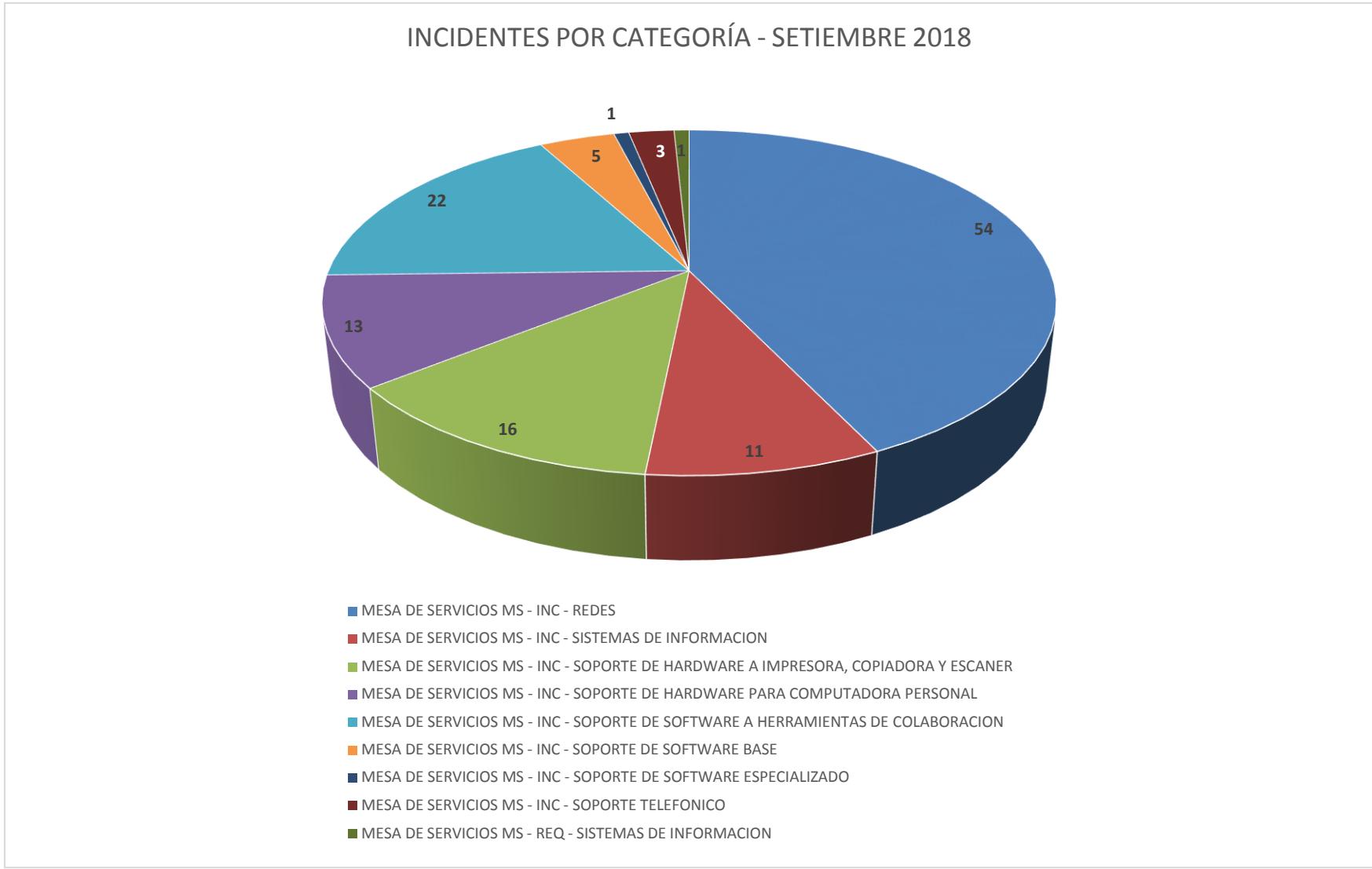
EVALUACIÓN POSTERIOR A LA AUDITORÍA DE SISTEMAS (Post Test)

Población = 185 incidentes
Muestra = 126 incidentes
Mes de aplicación: setiembre 2018

INCIDENTES POR CATEGORÍA - SETIEMBRE 2018

SERVICIO	CATEGORÍA	CANTIDAD DE TICKETS SETIEMBRE
MESA DE SERVICIOS	MS - INC - REDES	54
	MS - INC - SISTEMAS DE INFORMACIÓN	11
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCANER	16
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	13
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	22
	MS - INC - SOPORTE DE SOFTWARE BASE	5
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	1
	MS - INC - SOPORTE TELEFONICO	3
	MS - REQ - SISTEMAS DE INFORMACION	1
TOTAL		**126**

Fuente: Incidentes por categoría – setiembre 2018


INCIDENTES POR CATEGORÍA - SETIEMBRE 2018
1
5
3
1
22
54
13
16
11
MESA DE SERVICIOS MS - INC - REDES
MESA DE SERVICIOS MS - INC - SISTEMAS DE INFORMACION
MESA DE SERVICIOS MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCANER
MESA DE SERVICIOS MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL
MESA DE SERVICIOS MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACION
MESA DE SERVICIOS MS - INC - SOPORTE DE SOFTWARE BASE
MESA DE SERVICIOS MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO
MESA DE SERVICIOS MS - INC - SOPORTE TELEFONICO
MESA DE SERVICIOS MS - REQ - SISTEMAS DE INFORMACION

INCIDENTES POR SUBCATEGORÍA - SETIEMBRE 2018

SERVICIO	CATEGORÍA Y SUBCATEGORÍA	CANTIDAD DE INCIDENTES SETIEMBRE
MESA DE SERVICIOS	**MS - INC - REDES**	**54**
	RED LAN INSTITUCIONAL	54
	MS - INC - SISTEMAS DE INFORMACIÓN	**11**
	JUEGOS DEPORTIVOS ESCOLARES	1
	PASSPORT	2
	Portal MINEDU	1
	SINAD	3
	SISTEMA DE CONVOCATORIA CAS	1
	SUP	1
	VIATICOS DESKTOP	1
	WASICHAY	1
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**16**
	IMPRESORA INYECCIÓN	2
	IMPRESORA LÁSER	4
	MULTIFUNCIONAL LÁSER	9
	SCANNER	1
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**13**
	LAPTOP	2
	LECTOR AIO	1
	PC	8
	PC AIO	1

	TECLADO	1
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**22**
	ALOJAMIENTO DE ARCHIVOS	1
	CORREO ELECTRÓNICO	15
	INTERNET	6
	MS - INC - SOPORTE DE SOFTWARE BASE	**5**
	ANTIVIRUS	2
	OFIMATICA - OFFICE	1
	SISTEMA OPERATIVO	2
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**1**
	PROGRAMACIÓN	1
	MS - INC - SOPORTE TELEFÓNICO	**3**
	TELEFONO IP	3
	MS - REQ - SISTEMAS DE INFORMACIÓN	**1**
	SUP	1
TOTAL		**126**

Fuente: Incidentes por subcategoría – setiembre 2018

INCIDENTES REGISTRADOS INCORRECTAMENTE - SETIEMBRE 2018

SERVICIO	REGISTRO	CATEGORÍA Y SUBCATEGORÍA	CANTIDAD DE INCIDENTES SETIEMBRE
MESA DE SERVICIOS	CORRECTO	**MS - INC - REDES**	**54**
		RED LAN INSTITUCIONAL	54
		MS - INC - SISTEMAS DE INFORMACIÓN	**11**
		JUEGOS DEPORTIVOS ESCOLARES	1
		PASSPORT	2
		Portal MINEDU	1
		SINAD	3
		SISTEMA DE CONVOCATORIA CAS	1
		SUP	1
		VIATICOS DESKTOP	1
		WASICHAY	1
		MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**16**
		IMPRESORA INYECCIÓN	2
		IMPRESORA LÁSER	4
		MULTIFUNCIONAL LÁSER	9
		SCANNER	1
		MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**13**
		LAPTOP	2
		LECTOR AIO	1
		PC	8
		PC AIO	1
		TECLADO	1

		MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**22**
		ALOJAMIENTO DE ARCHIVOS	1
		CORREO ELECTRÓNICO	15
		INTERNET	6
		MS - INC - SOPORTE DE SOFTWARE BASE	**5**
		ANTIVIRUS	2
		OFIMATICA - OFFICE	1
		SISTEMA OPERATIVO	2
		MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**1**
		PROGRAMACION	1
		MS - INC - SOPORTE TELEFÓNICO	**3**
		TELEFONO IP	3
	INCORRECTO	**MS - REQ - SISTEMAS DE INFORMACIÓN**	**1**
		SUP	1
TOTAL			**126**

Fuente: Incidentes registrado incorrectamente – setiembre 2018

- En este reporte realizado en el periodo de setiembre 2018 se evidencia que la cantidad de incidentes mal registrados se mantiene; no obstante, el mal registro no recae sobre la misma categoría, en esta oportunidad el agente de atención de nivel 1 registro una petición como incidentes en la categoría de Sistemas de Información, específicamente para el Sistema Único de Planillas. Como en el periodo anterior, no se aplicó correctamente el procedimiento para la gestión de incidentes perjudicando los acuerdos de niveles de servicio y en consecuencia se genera demora en la atención, debido a que las peticiones de servicio tienen un tiempo holgado de atención, ya que estos son programados y coordinados con el usuario; Además, el nivel de satisfacción del usuario se afecta directamente ante la percepción de demora en la atención.

INCIDENTES MAL DIAGNOSTICADOS - SETIEMBRE 2018

SERVICIO	CATEGORÍA Y SUBCATEGORÍA	DIAGNÓSTICO		CANTIDAD DE INCIDENTES SETIEMBRE
		CORRECTO	INCORRECTO	
MESA DE SERVICIOS	**MS - INC - REDES**	**39**	**15**	**54**
	RED LAN INSTITUCIONAL	39	15	54
	MS - INC - SISTEMAS DE INFORMACIÓN	**2**	**9**	**11**
	JUEGOS DEPORTIVOS ESCOLARES		1	1
	PASSPORT		2	2
	Portal MINEDU		1	1
	SINAD		3	3
	SISTEMA DE CONVOCATORIA CAS	1		1
	SUP		1	1
	VIATICOS DESKTOP	1		1
	WASICHAY		1	1
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**8**	**8**	**16**
	IMPRESORA INYECCIÓN	2		2
	IMPRESORA LÁSER	3	1	4
	MULTIFUNCIONAL LÁSER	3	6	9
	SCANNER		1	1
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**9**	**4**	**13**
	LAPTOP	1	1	2
	LECTOR AIO		1	1
	PC	7	1	8

	PC AIO	1		1
	TECLADO		1	1
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**7**	**15**	**22**
	ALOJAMIENTO DE ARCHIVOS		1	1
	CORREO ELECTRÓNICO	5	10	15
	INTERNET	2	4	6
	MS - INC - SOPORTE DE SOFTWARE BASE	**3**	**2**	**5**
	ANTIVIRUS		2	2
	OFIMATICA - OFFICE	1		1
	SISTEMA OPERATIVO	2		2
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO		**1**	**1**
	PROGRAMACIÓN		1	1
	MS - INC - SOPORTE TELEFÓNICO	**1**	**2**	**3**
	TELEFONO IP	1	2	3
	MS - REQ - SISTEMAS DE INFORMACIÓN		**1**	**1**
	SUP		1	1
TOTAL		**69**	**57**	**126**

Fuente: Incidentes mal diagnosticados – setiembre 2018

- Se valida que posterior a la auditoria de sistemas la cantidad de incidentes mal diagnosticados se redujo en 6%, siendo los porcentajes de correctos 55% y los incorrectos 45%. Para este caso, se valida que la auditoria de sistemas afecta de manera positiva en el Diagnostico de incidentes en proceso de atención al usuario en la Unidad de Servicio de Atención al Usuario – USAU de la Oficina de Tecnologías de la Información y Comunicación – OTIC del Ministerio de Educación.

TIEMPO DE RESOLUCIÓN DE INCIDENTES - SETIEMBRE 2018

SERVICIO	TIEMPO DE RESOLUCIÓN POR CATEGORÍA	CANTIDAD DE INCIDENTES JUNIO
MESA DE SERVICIOS	**MS - INC - REDES**	**54**
	00:00:00	4
	00:00:13	1
	00:00:43	1
	00:05:15	1
	00:15:28	1
	00:23:16	1
	00:24:11	1
	00:24:46	1
	00:33:30	1
	00:35:13	1
	00:36:13	1
	00:36:28	1
	00:46:02	1
	00:47:09	1
	00:49:41	1
	00:56:54	1
	00:59:03	1
	01:01:08	1
	01:12:48	1
	01:16:53	1
	01:24:13	1
	01:55:31	1
	02:02:43	1
	02:03:31	1

	02:24:43	1
	02:43:05	1
	03:09:05	1
	03:33:26	1
	03:40:37	1
	03:42:30	1
	03:43:02	1
	03:45:50	1
	04:06:00	1
	04:22:43	1
	04:32:57	1
	04:34:27	1
	05:14:42	1
	05:21:46	1
	05:32:51	1
	05:51:31	1
	06:33:21	1
	06:39:32	1
	06:57:16	1
	07:27:45	1
	07:32:12	1
	07:32:33	1
	08:31:36	1
	10:18:39	1
	24:08:00	1
	243:02:51	1
	30:05:08	1
	MS - INC - SISTEMAS DE INFORMACIÓN	**11**

	00:00:00	2
	00:22:14	1
	01:25:20	1
	04:05:15	1
	13:42:51	1
	21:50:15	1
	26:10:36	1
	31:01:20	1
	36:09:40	1
	54:08:06	1
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**16**
	00:00:00	4
	00:42:02	1
	00:57:25	1
	00:57:41	1
	01:01:03	1
	01:07:35	1
	01:07:49	1
	01:31:01	1
	04:56:12	1
	05:02:01	1
	09:26:28	1
	12:33:27	1
	88:19:26	1
	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**13**
	00:00:00	5

	01:22:25	1
	01:47:05	1
	01:49:24	1
	02:27:22	1
	02:45:06	1
	03:03:06	1
	09:58:33	1
	133:15:33	1
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**22**
	00:00:08	1
	00:00:10	1
	00:01:27	1
	00:02:15	1
	00:06:17	1
	00:26:01	1
	00:32:22	1
	00:42:44	1
	01:01:15	1
	01:01:48	1
	01:11:15	1
	01:14:50	1
	01:17:00	1
	01:27:21	1
	01:30:55	1
	01:36:32	1
	01:53:38	1
	03:39:41	1

	04:03:53	1
	04:27:14	1
	04:34:52	1
	07:03:35	1
	MS - INC - SOPORTE DE SOFTWARE BASE	**5**
	00:00:00	1
	01:15:06	1
	01:30:58	1
	03:10:37	1
	124:53:06	1
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO	**1**
	08:00:42	1
	MS - INC - SOPORTE TELEFÓNICO	**3**
	00:00:09	1
	09:53:31	1
	50:55:11	1
	MS - REQ - SISTEMAS DE INFORMACIÓN	**1**
	150:18:38	1
TOTAL		**126**

Fuente: Tiempo de resolución de incidentes – setiembre 2018

- Se valida en el reporte del periodo setiembre 2018 que los tiempos de resolución de incidentes se redujo considerablemente (más del 50% aproximadamente para los extremos), teniendo en cuenta que el tiempo promedio de resolución en junio 2018 de 8 horas y para el presente periodo setiembre 2018 de 6 horas en promedio. Asimismo, para el caso de tiempos extremos de resolución que estuvieron en 313 horas en promedio en el mes de junio 2018, para el presente periodo de setiembre 2018 los tiempos extremos de resolución fueron de 163 horas en promedio. Se valida que la auditoria de sistemas mejoró los tiempos de resolución de los incidentes en el proceso de atención al usuario en la Unidad de Atención al Usuario – USAU de la Oficina de Tecnologías de la Información y Comunicación – OTIC del Ministerio de Educación.

TIEMPO DE RESOLUCIÓN POR DIAGNÓSTICO - SETIEMBRE 2018

SERVICIO	TIEMPO DE RESOLUCIÓN POR CATEGORÍA	DIAGNÓSTICO		CANTIDAD DE TICKETS JUNIO	CANTIDAD DE INCIDENETS DESBORDADOS
		CORRECTO	INCORRECTO		
MESA DE SERVICIOS	**MS - INC - REDES**	**39**	**15**	**54**	**4**
	00:00:00	4		4	
	00:00:13	1		1	
	00:00:43	1		1	
	00:05:15	1		1	
	00:15:28	1		1	
	00:23:16	1		1	
	00:24:11	1		1	
	00:24:46	1		1	
	00:33:30		1	1	
	00:35:13	1		1	
	00:36:13	1		1	
	00:36:28	1		1	
	00:46:02	1		1	
	00:47:09		1	1	
	00:49:41	1		1	
	00:56:54		1	1	
	00:59:03	1		1	
	01:01:08	1		1	
	01:12:48	1		1	
	01:16:53		1	1	
	01:24:13	1		1	
	01:55:31		1	1	
	02:02:43	1		1	

	02:03:31	1		1	
	02:24:43		1	1	
	02:43:05		1	1	
	03:09:05	1		1	
	03:33:26		1	1	
	03:40:37	1		1	
	03:42:30	1		1	
	03:43:02	1		1	
	03:45:50	1		1	
	04:06:00	1		1	
	04:22:43	1		1	
	04:32:57		1	1	
	04:34:27	1		1	
	05:14:42	1		1	
	05:21:46	1		1	
	05:32:51	1		1	
	05:51:31	1		1	
	06:33:21	1		1	
	06:39:32		1	1	
	06:57:16	1		1	
	07:27:45	1		1	
	07:32:12	1		1	
	07:32:33	1		1	
	08:31:36		1	1	
	10:18:39		1	1	
	24:08:00		1	1	
	243:02:51		1	**1**	
	30:05:08		1	1	

	MS - INC - SISTEMAS DE INFORMACIÓN	**2**	**9**	**11**	
	00:00:00	2		2	
	00:22:14		1	1	
	01:25:20		1	1	
	04:05:15		1	1	
	13:42:51		1	1	
	21:50:15		1	1	
	26:10:36		1	1	
	31:01:20		1	1	
	36:09:40		1	1	
	54:08:06		1	1	
	MS - INC - SOPORTE DE HARDWARE A IMPRESORA, COPIADORA Y ESCÁNER	**8**	**8**	**16**	
	00:00:00	2	2	4	
	00:42:02	1		1	
	00:57:25	1		1	
	00:57:41	1		1	
	01:01:03	1		1	
	01:07:35		1	1	
	01:07:49	1		1	
	01:31:01		1	1	
	04:56:12		1	1	
	05:02:01	1		1	
	09:26:28		1	1	
	12:33:27		1	1	
	88:19:26		1	1	

	MS - INC - SOPORTE DE HARDWARE PARA COMPUTADORA PERSONAL	**9**	**4**	**13**	
	00:00:00	4	1	5	
	01:22:25	1		1	
	01:47:05		1	1	
	01:49:24	1		1	
	02:27:22		1	1	
	02:45:06	1		1	
	03:03:06	1		1	
	09:58:33	1		1	
	133:15:33		1	**1**	
	MS - INC - SOPORTE DE SOFTWARE A HERRAMIENTAS DE COLABORACIÓN	**7**	**15**	**22**	
	00:00:08	1		1	
	00:00:10	1		1	
	00:01:27	1		1	
	00:02:15		1	1	
	00:06:17	1		1	
	00:26:01		1	1	
	00:32:22		1	1	
	00:42:44		1	1	
	01:01:15		1	1	
	01:01:48		1	1	
	01:11:15		1	1	
	01:14:50		1	1	
	01:17:00	1		1	
	01:27:21		1	1	

	01:30:55	1		1
	01:36:32		1	1
	01:53:38		1	1
	03:39:41		1	1
	04:03:53	1		1
	04:27:14		1	1
	04:34:52		1	1
	07:03:35		1	1
	MS - INC - SOPORTE DE SOFTWARE BASE	**3**	**2**	**5**
	00:00:00		1	1
	01:15:06	1		1
	01:30:58	1		1
	03:10:37	1		1
	124:53:06		1	**1**
	MS - INC - SOPORTE DE SOFTWARE ESPECIALIZADO		**1**	**1**
	08:00:42		1	1
	MS - INC - SOPORTE TELEFÓNICO	**1**	**2**	**3**
	00:00:09	1		1
	09:53:31		1	1
	50:55:11		1	1
	MS - REQ - SISTEMAS DE INFORMACIÓN		**1**	**1**
	150:18:38		1	**1**
TOTAL		**69**	**57**	**126**

Fuente: Tiempo de resolución por diagnóstico – Setiembre 2018

- En el reporte del periodo setiembre 2018 se valida que los tiempos extremos de resolución de incidentes se mantienen sobre los incidentes mal diagnosticadas; sin embargo, a las cantidades de ocurrencias se redujo de 4 a 6 casos identificados. Quiere decir que la auditoria de sistemas realizada al proceso de atención al usuario permitió disminuir la cantidad de ocurrencias con tiempos de resolución extremo; para obtener dicho resultado se aplicaron controles procedimentales que permitieron mejorar los diagnósticos.