

**PROGRAMA DE ESTUDIO DE ARQUITECTURA DE PLATAFORMAS Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN**

**ORGANIZACIÓN DE RECURSOS**

**CASOS METODOLOGIA ITIL – MAGERIT**

**INTEGRANTES**

Collantes Portilla Candy

Montalvan Pintado Edilsa

Nanfuñay Carrion Javier

Neyra Quesquen Renzo

**Chiclayo , Abril del 2023**

**EMPRESA DE OUTSOURCING DE TI**

La empresa ofrece sus servicios a clientes de diferentes sectores económicos, actualmente posee tres clientes con contratos de soporte.

**PROBLEMA**

Su responsabilidad consiste en asesorar a esta empresa para que saque provecho de una implementación de ITIL para la gestión de los Servicios de TI que presta.

1. **Identifique las diversas etapas del ciclo de servicio en la empresa.**

La empresa de outsourcing de TI tiene un ciclo de servicio con las siguientes etapas:

* 1. Estrategia de servicio: La empresa debe definir su enfoque estratégico, establecer objetivos claros y acordes a las necesidades de los clientes, identificar y priorizar los servicios que ofrecerá, establecer acuerdos de nivel de servicio y planificar su capacidad de recursos.
  2. Diseño de servicio: En esta etapa, la empresa diseña los servicios de TI que ofrecerá, asegurándose de que sean adecuados para satisfacer las necesidades del cliente y cumplir con los SLAs acordados. Esto incluye el diseño de la arquitectura de los servicios, la selección de herramientas y tecnologías, la definición de procesos y procedimientos, la identificación de riesgos y la planificación de la continuidad del servicio.
  3. Transición de servicio: En esta etapa, la empresa implementa los servicios diseñados, los prueba y los pone en marcha en el entorno del cliente. Se lleva a cabo la gestión de cambios y se asegura la calidad de los servicios antes de su entrega.
  4. Operación de servicio: En esta etapa, la empresa presta los servicios a los clientes, monitorea su desempeño y cumple con los SLAs establecidos. La gestión de incidentes, problemas y eventos son procesos críticos en esta etapa.
  5. Mejora continua del servicio: En esta etapa, la empresa analiza los resultados de los servicios prestados y realiza mejoras en los servicios, procesos y procedimientos, con el objetivo de lograr una mejora continua de la calidad del servicio.

1. **Identifique los principales procesos que se llevan a cabo en los servicios de la empresa.**

La empresa de outsourcing de TI lleva a cabo los siguientes procesos en la prestación de sus servicios:

* 1. Gestión de incidentes: Este proceso se encarga de la gestión de los incidentes reportados por los clientes, con el objetivo de restaurar el servicio en el menor tiempo posible.
  2. Gestión de problemas: Este proceso se encarga de la gestión de los problemas subyacentes que pueden estar causando incidentes, con el objetivo de evitar su recurrencia en el futuro.
  3. Gestión de cambios: Este proceso se encarga de la gestión de los cambios en la infraestructura de TI, con el objetivo de minimizar el impacto de los cambios en los servicios prestados.
  4. Gestión de configuración: Este proceso se encarga de mantener un registro actualizado de la configuración de la infraestructura de TI, con el objetivo de tener información precisa sobre los elementos que componen los servicios prestados.
  5. Gestión de nivel de servicio: Este proceso se encarga de la gestión de los acuerdos de nivel de servicio (SLAs) acordados con los clientes, con el objetivo de asegurar la calidad del servicio prestado y cumplir con los compromisos adquiridos.

1. **Cree un esquema de implementación de ITIL para esta empresa.**

**ESTRATEGIA DE SERVICIO**

La empresa, aunque preste a sus clientes servicios, mediante lo analizado no le saca su máximo provecho, es por ello que nosotros hemos propuesto las siguientes estrategias de servicios en la cual la empresa pueda tener una mejora en los servicios que brinda.

1. Establecer una comunicación clara, efectiva y de confianza: La empresa debe tener una comunicación clara, efectiva y de confianza con sus clientes en todo momento. Esto incluye establecer canales de comunicación abiertos y efectivos, tales como correo electrónico, teléfono, chat en línea, entre otros, y tener un equipo de soporte dedicado para responder a las consultas y preguntas de los clientes.
2. Implementar un sistema de seguimiento de tickets: Es importante contar con una herramienta que permita el registro y seguimiento de los tickets de soporte técnico. Esto ayuda a mantener un registro de las solicitudes de los clientes, su estatus y el tiempo de resolución.
3. Garantizar la calidad: La empresa debe asegurarse de que sus servicios sean de alta calidad y cumplan con los estándares de la industria.
4. Mantenerse actualizado: La empresa debe estar al día con las últimas tendencias y tecnologías de la industria para poder ofrecer soluciones innovadoras y de vanguardia a sus clientes.
5. Ser flexible: La empresa debe ser capaz de adaptarse rápidamente a cualquier cambio en las necesidades del cliente, y estar preparada para hacer ajustes en su servicio en consecuencia.
6. Ofrecer soporte remoto y presencial: Es importante ofrecer tanto soporte remoto como presencial, dependiendo de las necesidades del cliente. Esto permite resolver problemas técnicos de manera rápida y efectiva, sin importar la ubicación del cliente o del equipo.
7. Implementar un programa de mantenimiento preventivo: Es importante contar con un programa de mantenimiento preventivo que permita mantener los equipos en buen estado y evitar problemas técnicos. Esto implica realizar revisiones periódicas a los equipos, limpieza, lubricación, reemplazo de piezas defectuosas, entre otros.

**DISEÑO DE SERVICIO**

* Se Implementa una línea de ayuda en la que los clientes pueden comunicarse para que los usuarios reciban ayuda y orientación de manera rápida y efectiva.

Se van a integrar las herramientas de seguimiento de tickets, además de la gestión de incidentes para saber cuál es el estatus de cada solicitud que el cliente requiere.

* Se establecerán estándares de calidad para el servicio de TI, lo que significa que se deben definir los objetivos y expectativas de calidad que se esperan alcanzar.

Se implementará un sistema de monitoreo y seguimiento, para asegurar de se están entregando de manera consistente y cumplen con los estándares de calidad.

* Al tratarse de una empresa dedicada a los servicios de TI, debería mantenerse en constante actualización, tanto de software como de los avances tecnológicos en cuanto a hardware se refiere, por lo tanto, se programará capacitaciones al personal que estará encargado de esta tarea
* Implementar sistemas de servicios u opciones de pago que estén al alcance del cliente, esto permitirá la elección del servicio que mejor se adapte a las necesidades de los clientes, además de proporcionar al cliente negociar más profundamente con la empresa.
* Uno de los servicios que proporciona la empresa es el mantenimiento de hardware, por eso es importante crear un plan de mantenimiento preventivo para cada cliente, teniendo en cuenta el uso que éste le da a sus equipos, así como otros parámetros que nos permitan mantener el hw en un buen estado, y evitar en lo posible que llegue a recibir el mantenimiento del tipo correctivo.

**TRANSICIÓN DEL SERVICIO**

* Mediante los sistemas, planes y estándares mencionados anteriormente, se realizarán las respectivas capacitaciones a los colaboradores de la empresa para que se familiaricen con los sistemas, de esta manera se realizarán las pruebas con el uso que le darán los miembros de la organización.

**OPERACIÓN DEL SERVICIO**

* Con las pruebas y capacitaciones a los colaboradores de la empresa ya finalizadas, se ponen en marcha las implementaciones de los sistemas, planes y estándares en toda la empresa.

**MEJORA CONTINUA DEL SERVICIO**

* Recopilar información en encuestas sobre el desempeño que tiene la empresa de parte de los trabajadores y del sistema implementado, esto permitirá que, en base a la información obtenida, se mejore tanto la atención al cliente como el sistema de la empresa.

1. **¿Qué ventajas obtendría la empresa de implantar ITIL?**
   1. Mejora la calidad de los servicios de TI ofrecidos, aumentando la satisfacción de los clientes.
   2. Establecer procesos claros y estructurados para la gestión de incidentes, problemas y cambios, reduciendo el tiempo de resolución de los mismos.
   3. Permite una mejor planificación y gestión de los recursos de TI de la empresa, optimizando su uso y reduciendo costos.
   4. Proporciona una visión clara y completa de los servicios de TI ofrecidos, facilitando la toma de decisiones estratégicas.
   5. Permite una gestión más eficiente y proactiva de la infraestructura de TI, reduciendo el riesgo de fallos y aumentando la disponibilidad de los servicios.
2. **Defina cuál sería la documentación mínima requerida para el control de la gestión de la empresa.**

* Manuales de usuario: documentos que describen cómo utilizar los productos o servicios de la empresa.
* Planes de contingencia: documentos que establecen los procedimientos de emergencia para situaciones imprevistas, como desastres naturales o interrupciones del negocio.
* Informes financieros: documentos que detallan la situación financiera de la empresa, como estados de resultados, balances y flujo de efectivo.
* Registros de empleados: estos documentos incluyen información personal y de trabajo de los empleados, como contratos, registros de horas trabajadas y evaluaciones de desempeño.
* Registros de clientes: estos documentos incluyen información sobre los clientes, como nombres, direcciones y detalles de contacto.
* Libros de actas: estos documentos incluyen registros de las decisiones tomadas en reuniones de la junta directiva, comités y otras reuniones importantes, y se utilizan para garantizar que se tomen decisiones informadas y se mantenga la transparencia.
* Registros de proveedores: estos documentos incluyen información sobre los proveedores de la empresa, como los contratos y los acuerdos de nivel de servicio, y se utilizan para garantizar que la empresa cumpla con sus compromisos con los proveedores.

1. **Establezca algunas herramientas de software que puedan ser útiles para la implementación de ITIL**

Algunas herramientas de software que pueden ser útiles para la implementación de ITIL son:

1. Herramientas de gestión de servicios de TI, como ServiceNow, BMC Remedy, HP Service Manager, entre otras, que pueden ayudar a automatizar procesos y proporcionar una visión unificada de los servicios y activos de TI.
2. Herramientas de monitoreo y gestión de eventos, como Nagios, Zabbix, Splunk, entre otras, que pueden ayudar a monitorear el desempeño de los servicios y activos de TI, detectar problemas y generar alertas en tiempo real.
3. Herramientas de gestión de cambios, como JIRA, GitLab, entre otras, que pueden ayudar a gestionar los cambios en los servicios de TI de manera controlada y minimizando el riesgo.
4. Herramientas de gestión de configuración, como Puppet, Chef, Ansible, entre otras, que pueden ayudar a identificar, registrar y controlar los componentes de la infraestructura de TI.
5. Herramientas de gestión de proyectos, como Asana, Trello, entre otras, que pueden ayudar a gestionar proyectos relacionados con la implementación de ITIL y monitorear el progreso y el cumplimiento de plazos y objetivos.

***CASO PROPUESTO DE MAGERIT***

ESPOL es una institución de educación superior de gran prestigio en la ciudad de Guayaquil, cuya misión es “Formar profesionales de excelencia, socialmente responsables, líderes, emprendedores, con principios y valores morales y éticos, que contribuyan al desarrollo científico, tecnológico, social, económico, ambiental y político del país; y, hacer investigación, innovación, transferencia de tecnología y extensión de calidad para servir a la sociedad”. Y su visión es “Ser líder y referente de la Educación….

1. Identifica el nivel de riesgo en que se encuentran los activos de GTSI y trata de minimizarlos con las respectivas salvaguardias.

|  |  |  |
| --- | --- | --- |
| **Amenaza** | **Activo** | **Riesgo** |
|  |
| Incendio y Terremoto | Servidores | Medio |  |
| Equipos de Comunicaciones | Medio |  |
|  |
| Computador de personal | Medio |  |
| Sistemas académicos, financieros y administrativos | Medio |  |
|  |
| Almacenamiento – bases de datos | Medio |  |
|  |
| Correo electrónico | Medio |  |
| Virtualización | Medio |  |
| Internet | Medio |  |
| Red alámbrica | Medio |  |
| Enlace con proveedor | Medio |  |
| UPS | Medio |  |
| Generador eléctrico | Medio |  |
| Equipos de climatización | Medio |  |
| Cableado eléctrico | Medio |  |
| Centro de datos | Medio |  |
| Cuarto de rack | Medio |  |
| Equipo de desarrollo | Medio |  |
| Equipo técnico | Medio |  |
| Administradores | Medio |  |
| Falla de generador eléctrico | Servidores | Medio |  |
| Equipos de comunicaciones | Medio |  |
| Agotamiento de recursos | Almacenamiento – bases de datos | Medio |  |
| Falla de equipos de climatización | UPS | Alto |  |
| Equipos de climatización | Alto |  |
| Acceso no autorizado | Servidores | Alto |  |
| Equipos de comunicaciones | Alto |  |
| Sistemas académicos, financieros y administrativos | Alto |  |
| Almacenamiento – bases de datos | Medio |  |
| Correo electrónico | Alto |  |
| Virtualización | Alto |  |
| Centro de datos | Medio |  |
| Cuarto de rack | Medio |  |
| Robo | Servidores | Bajo |  |
| Equipos de comunicaciones | Bajo |  |
| Computador de personal | Bajo |  |
| Desconexión Física o lógica | Equipos de comunicaciones | Medio |  |
| Almacenamiento – bases de datos | Bajo |  |
| Correo electrónico | Medio |  |
| Virtualización | Medio |  |
| Internet | Alto |  |
| Enlace con proveedor | Alto |  |
| Cableado eléctrico | Medio |  |
| Fuga de información | Equipo de desarrollo | Alto |  |
| Equipo técnico | Alto |  |
| Administradores | Alto |  |
| Malware | Computador de personal | Alto |  |

Las amenazas con un nivel alto de riesgo son:

* + - * Acceso no autorizado. - Afecta de forma directa a la integridad y confidencialidad de la información, debido a varios factores: las contraseñas de las cuentas con privilegios no se cambian de forma periódica, algunas no cumplen los requisitos de una contraseña compleja, no existe una directiva de control del acceso remoto, aún siguen activas las cuentas de ex empleados y tampoco se comprueba de forma periódica la configuración de los cortafuegos.
      * Desconexión física o lógica. - Afecta a la disponibilidad de la información y es

debido a que de forma continua se presentan caídas en el enlace con el proveedor de internet, lo cual provoca problemas en los demás servicios dependientes del internet. Referente a la desconexión física, existe esta amenaza al no tener armarios con puertas en el centro de datos ni en los cuartos de red, y por esto las conexiones de los equipos de comunicación y servidores se encuentran expuestas.

* + - * Fuga de información. - Afecta a la confidencialidad de la información al no existir un proceso formal de salida de empleados, ni una política sobre el almacenamiento de información institucional en los computadores personales.
      * Malware. - Afecta la integridad de la información almacenada en los servidores y equipos del personal que no cuentan con un software antimalware.
      * Fallas de equipos de climatización. - Afecta la disponibilidad de la información que es procesada en los centros de datos y cuartos de rack, cuando se presentan problemas con los equipos de climatización, porque han superado el ciclo de servicio y requieren ser renovados.

|  |  |
| --- | --- |
| **Riesgos** | **Salvaguardas** |
| Incendio y Terremoto | Instalación de sistemas contra incendio |
| Instalación de alarmas contra incendio |
| Uso y mantenimiento de extintores |
| Desarrollo de plan de emergencia ante incendios |
| Desarrollo de plan de contingencia ante desastres |
| Realizar simulacros de forma periódica |
| Falla de generador eléctrico | Mantenimiento periódico de generador eléctrico |
| Falla de equipos de climatización | Mantenimiento de equipos de climatización |
| Adquirir nuevos equipos de climatización |
| Agotamiento de recursos | Mantenimiento preventivo de servidores |
| Revisión de directiva de copias de seguridad de forma regular |
| Monitoreo de recursos de los equipos críticos |
| Desconexión Física o lógica | Asegurar los equipos de comunicaciones y servidores en armarios cerrados |
| Robo | Uso de cables de seguridad para computadores de personal y portátiles |
| Virus | Instalación de antivirus en servidores |
| Instalación de antivirus en equipos de personal |
| Actualizar periódicamente la base de datos de los antivirus |
| Malware | Instalación de antimalware en servidores |
| Instalación de antimalware en equipos de personal |
| Errores de configuración | Realizar pruebas de actualizaciones previo a la instalación |
| Pruebas periódicas del cortafuegos |
| Acceso no autorizado | Establecer controles de acceso físico |
| Analizar directivas de cortafuegos con regularidad |
| Implementación de sistema de detección de intrusos |
| Asignar cuentas para la administración de sistemas |
| Implementar directivas de contraseñas complejas |
| Fuga de información | Implementar cifrado de datos |
| Contratar personal responsable de la seguridad |
| Solicitar historial de personal antes de ser contratado |
| Dar charlas al personal referente a la seguridad |

1. Analiza el caso en las fases de MAGERIT
   1. **Activos**

* Hardware:
  + Servidores
  + Equipos de comunicaciones
  + Computadores personales
* Software:
  + Sistemas implementados por la institución
  + Almacenamiento – Base de datos
  + Correo electrónico
  + Virtualización
* Comunicaciones:
  + Internet
  + Red cableada
  + Enlace con el proveedor
* Equipo auxiliar:
  + UPS
  + Generador eléctrico
  + Equipo de climatización
  + Cableado eléctrico
* Instalaciones:
  + Centro de datos
  + Cuarto de Rack
* Personal:
  + Equipo de desarrollo
  + Equipo técnico
  + Administradores
  1. **Amenazas**
  + Incendio y Terremoto
  + Falla de generador eléctrico
  + Agotamiento de recursos
  + Falla de equipos de climatización
  + Acceso no autorizado
  + Robo
  + Desconexión Física o lógica
  + Fuga de información
  + Malware
  1. **Riesgo**

|  |  |
| --- | --- |
| **Amenaza** | **Riesgo** |
|  |
| Incendio y Terremoto | Medio |  |
| Falla de generador eléctrico | Medio |  |
| Agotamiento de recursos | Medio |  |
| Falla de equipos de climatización | Alto |  |
| Acceso no autorizado | Alto/Medio |  |
| Robo | Medio |  |
| Desconexión Física o lógica | Alto/Medio |  |
| Fuga de información | Alto |  |
| Malware | Alto |  |

* 1. **Salvaguardias**

|  |  |
| --- | --- |
| **Riesgos** | **Salvaguardas** |
| Incendio y Terremoto | Instalación de sistemas contra incendio |
| Instalación de alarmas contra incendio |
| Uso y mantenimiento de extintores |
| Desarrollo de plan de emergencia ante incendios |
| Desarrollo de plan de contingencia ante desastres |
| Realizar simulacros de forma periódica |
| Falla de generador eléctrico | Mantenimiento periódico de generador eléctrico |
|  |
| Falla de equipos de climatización | Mantenimiento de equipos de climatización |  |
| Adquirir nuevos equipos de climatización |  |
| Agotamiento de recursos | Mantenimiento preventivo de servidores |  |
| Revisión de directiva de copias de seguridad de forma regular |  |
| Monitoreo de recursos de los equipos críticos |  |
| Desconexión Física o lógica | Asegurar los equipos de comunicaciones y servidores en armarios cerrados |  |
| Robo | Uso de cables de seguridad para computadores de personal y portátiles |  |
| Virus | Instalación de antivirus en servidores |  |
| Instalación de antivirus en equipos de personal |  |
| Actualizar periódicamente la base de datos de los antivirus |  |
| Malware | Instalación de antimalware en servidores |  |
| Instalación de antimalware en equipos de personal |  |
| Errores de configuración | Realizar pruebas de actualizaciones previo a la instalación |  |
| Pruebas periódicas del cortafuegos |  |
| Acceso no autorizado | Establecer controles de acceso físico |  |
| Analizar directivas de cortafuegos con regularidad |  |
| Implementación de sistema de detección de intrusos |  |
| Asignar cuentas para la administración de sistemas |  |
| Implementar directivas de contraseñas complejas |  |
| Fuga de información | Implementar cifrado de datos |  |
| Contratar personal responsable de la seguridad |  |
| Solicitar historial de personal antes de ser contratado |  |
| Dar charlas al personal referente a la seguridad |  |