**Nombre Del Sistema de Información:**

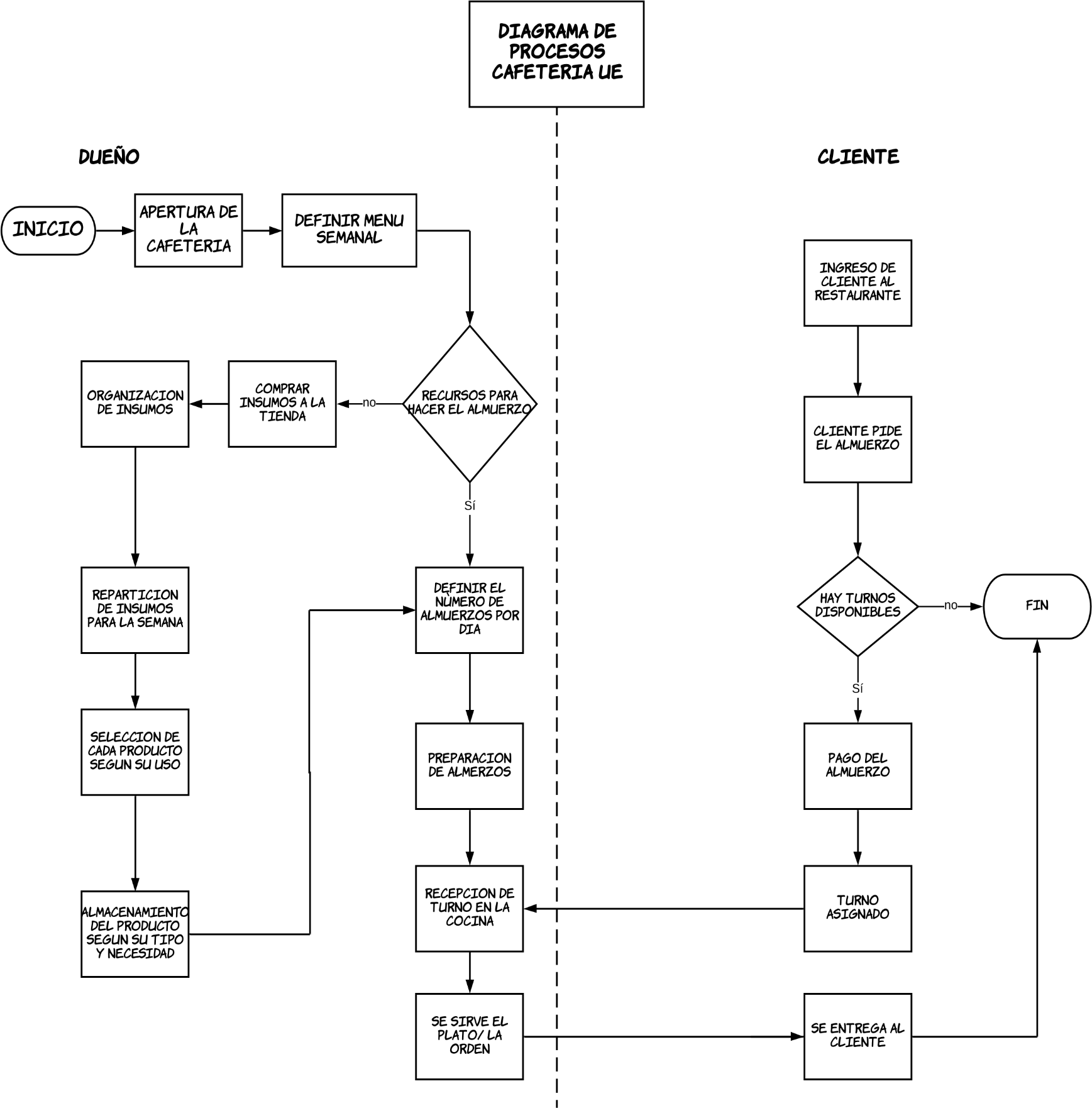
Easy Lunch.

**Tipo de Sistema de Información:**

Control Proceso Negocio.

**Análisis Pregunta Problema:**

En la cafetería de Uniempresarial es necesario implementar un sistema adecuado con el cual se organice la información, de acuerdo a los procesos actuales, que fomenten una mejor organización y evite los tiempo largos de espera, con el objetivo de prestar un mejor servicio a la hora del almuerzo. *¿Cómo implementar un sistema de información por medio de un dispositivo móvil o aplicación web que incluya opciones de menú y tiempos de entrega, logrando optimizar y mejorar el servicio?*



**Identificación de las Fronteras de Solución:**

El sistema de Información Easy Lunch va a interactuar con clientes de Uniempresarial ya sean administrativos, docentes y/o estudiantes.

Sistemas de Información Easy Lunch



EMPLEADOS

CLIENTES



ESTUDIANTES

ADMINISTRATIVOS

DOCENTES

Administrativos: Las personas que pertenecen a las áreas administrativas, en ocasiones necesitan que les lleven el almuerzo, para evitar que ellos tengan que gastar saldo de celular, podrían usar la aplicación que pertenezca al sistema de información y de esta manera pedir almuerzos para las horas en los que estos consideren estar disponibles.

Docentes: Los docentes llegan a tener responsabilidades con estudiantes o administrativos, tales como reuniones y resoluciones de conflictos, el sistema de información guarda el menú y la hora solicitados por el docente.

Estudiantes: Los estudiantes que suelen almorzar en la universidad, pueden asegurar que pedirán almuerzo y será más fácil para la cafetería preparar los alimentos del día y así evitarle a los demás las largas filas.

Empleados: Los trabajadores de la cafetería podrán ver los pedidos según el rol asignado para preparar las carnes de manera ordenada a la hora que piden el almuerzo y solo uno de ellos será el encargado de modificar el menú.

**Definición de las Restricciones:**

1. Económicas:

Posible aumento de costos en los almuerzos producidos para recuperar gradualmente la inversión del Sistema de Información.

1. Políticas:

* Indicar la manera en cómo la cafetería gestiona de manera segura el registro, ingreso y desvinculación, incluyendo temas de verificación de datos, aceptación de acuerdos de confidencialidad, recepción de acuerdos.
* Indica la manera en cómo la cafetería gestiona de manera segura y clasifica los alimentos de manera correcta, adicionalmente se debe explicar cómo se hace una correcta disposición de los alimentos cuando ya no se requieren o están en mal estado.
* Indica cómo la cafetería gestiona el acceso a sus sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza bruta, validando los datos completos para ingreso a los sistemas, empleando métodos para cifrar la información de acceso a través de la red, entre otros.
* Indica cómo realizar la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de las mismas. Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.
* Buen uso de la criptografía para garantizar la disponibilidad, integridad y confidencialidad de la información, así como también el correcto uso de las llaves criptográficas durante todo su ciclo de vida: creación, uso, recuperación, distribución, retiro y destrucción. Se pueden generar los siguientes procedimientos:
  1. Procedimientos de Controles Criptográficos**:** En este procedimiento deberá especificarse cómo se utilizará la criptografía dentro de los sistemas de información de la organización para garantizar su integridad, disponibilidad y confidencialidad.
  2. Debe especificarse la complejidad de los controles criptográficos a emplear, dependiendo de la criticidad de la información que circulará a través de la red o se encontrará alojada en un sistema determinado.
* Describir el ciclo de vida de las llaves criptográficas dentro de la entidad (si aplica), desde que se crean hasta que se distribuyen a cada usuario o aplicación de manera segura. Deben mencionarse aspectos como la creación de las llaves, obtención de certificados, almacenamiento seguro de las llaves, actualización o cambio, revocación y recuperación de llaves.
* Cómo realiza el control de cambios en la organización, los procesos de negocio y los sistemas de información de manera segura. Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa) entre otros.
* Indicar por medio de este procedimiento como realiza la protección contra códigos maliciosos teniendo en cuenta qué controles utiliza (hardware o software), cómo se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.
* Explicar la manera en que la entidad protege la información en las redes, indicando los controles de seguridad (como se cifran los datos a través de la red por ejemplo) que se aplican para acceder a la red cableada e inalámbrica, satelital, Entre otros. Con miras a proteger la privacidad de la información que circula a través de estos medios, también se debe incluir el uso de registros (logs) que permitan realizar seguimiento a acciones sospechosas.
* Indicar cómo realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.

Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento.

* Indicar cómo la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos tengan (es decir algún intermediario). Dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.
* Indicar cómo responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad. Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes De Continuidad) dependiendo de la criticidad de la información.
* Indicar la manera en que la entidad garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico.
* El procedimiento debe indicar los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal.
* Ley 23 de 1982: Derechos de Autor.
* Constitución Política de Colombia 1991: Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
* Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
* Ley 594 de 2000: Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
* Ley 603 de 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
* Ley 962 de 2005: Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
* Ley 1150 de 2007: Seguridad de la información electrónica en contratación en línea.
* Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
* Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y a las comunicaciones, entre otras disposiciones.
* Ley 1341 de 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
* Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley de 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la corrupción y se dictan otras disposiciones.
* Decreto 2364 de 2012: Firma electrónica.
* Decreto 2609 de 2012: Expediente electrónico.
* Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
* Decreto 2693 de 2012: Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
* Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
* Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
* Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
* Ley 1755 de 2015: Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Título II Capítulo I.

1. Técnicas:

* Describir cómo se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de la plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas.
* Pasos con los cuales los equipos son protegidos por la entidad. Se recomienda que este procedimiento indique cómo se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas, entre otros.
* Especificar cómo los activos son retirados de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos, entre otros).
* Especificar cómo se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, indicando los intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores o si existen seguros atados a los equipos y los mantenimientos sean requisitos. Se debe especificar el modo en que los mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.
* deberá describir cómo se realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (inhouse) o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad.

Se deben tener en cuenta el uso de ambientes de desarrollo, pruebas y producción para los sistemas de información.

* Indicar cómo realiza el control de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad,
* quienes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

1. El sistema de información Easy Lunch contará con los siguientes sistemas: Android, Google Chrome (Navegador Web), IOS.
2. Ambientales:

Se desarrollará un procedimiento de separación de ambientes que permita realizar una transición de los diferentes sistemas desde el ambiente de desarrollo hacia el de producción, con una implementación de un ambiente de pruebas para la aplicación y que estos tengan compatibilidad con el sistema.

1. Calendario y Recursos:

05-07-2019: Introducción al Sistema de Información.

12-07-2019: Desarrollo del diagrama de procesos.

19-07-2019: Análisis De la pregunta Problema.

26-07-2019 - 09-08-2019: Ingeniería De Requerimientos se trabajó en la planeación de la elicitación.

09-08-2019-16-08-2019: Análisis del Sistema de Información.

16-08-2019 - 23-08-2019: Especificación y Verificación del Sistema De Información.

30-08-2019 : Se trabajará en el UML.

06-09-2019: Se tendrá listo el diseño y con grandes avances.

**Identificación de las Necesidades**

* Usuarios de Uniempresarial.
* Sitio web o aplicación.
* Registro de usuario.
* Ingreso de sesión.
* Pedir y apartar almuerzo.
* Notificar a los usuarios sobre su almuerzo.
* Notificar a los dueños (cafetería) sobre informes de los pedidos del almuerzo.
* Registro de cuántos almuerzos se piden en un día.
* Evitar que los usuarios hagan pedidos sobre lo que no está establecido en el menú.
* Evitar la solicitud de almuerzos en horas no establecidas.
* Generar turnos digitales.
* Conexión de datos entre usuarios, solicitudes, cafetería y Uniempresarial.
* Controlar y autorizar el uso a usuarios registrados.
* Actualizaciones constantemente.
* Editar el menú desde la cafetería.
* Cancelar el pedido con 10 minutos de anterioridad.
* Consultar el menú con su debido precio.
* Alerta para cuando los productos se estén agotando y cuando esté listo el pedido.
* Búsqueda del menú del almuerzo del día.
* Registros diarios sobre los registros de almuerzos.