UNIVERSIDAD TECNOLÓGICA DE PUEBLA DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN- INGENIERÍA EN DESARROLLO Y GESTIÓN DE SOFTWARE

MATERIA:

ADMINISTRACIÓN DE BASE DE DATOS

Plan para desarrollar una aplicación segura

DOCENTE:

Luz María Pérez Sarmiento

ALUMNOS:

ANDRADE REYES JUSTINO JUAN CARLOS - UTP0002150

Domínguez Castillo Salvador Esteban -UTP0155077

GOIZ SARMIENTO MAURICIO - UTP0154599

Trujillo Alvarez Erik - UTP0155443

COYOTL MARCELINO ANGEL HOMAR - UTP0154813

8 ° A

FECHA: 29/01/2024

ÍNDICE

1. Plan de capacitación

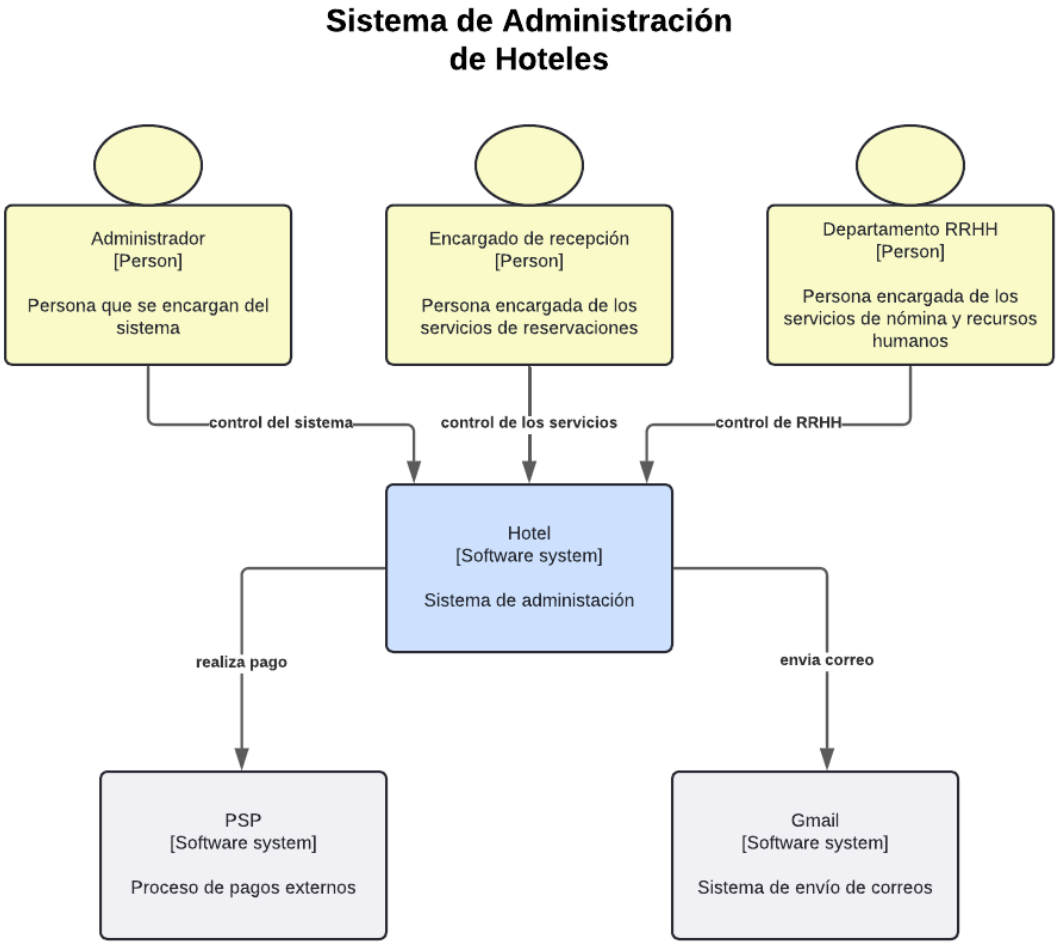
La forma en que se realizará la capacitación en materia de seguridad será a través de cursos en línea, quedando como cronograma el siguiente:

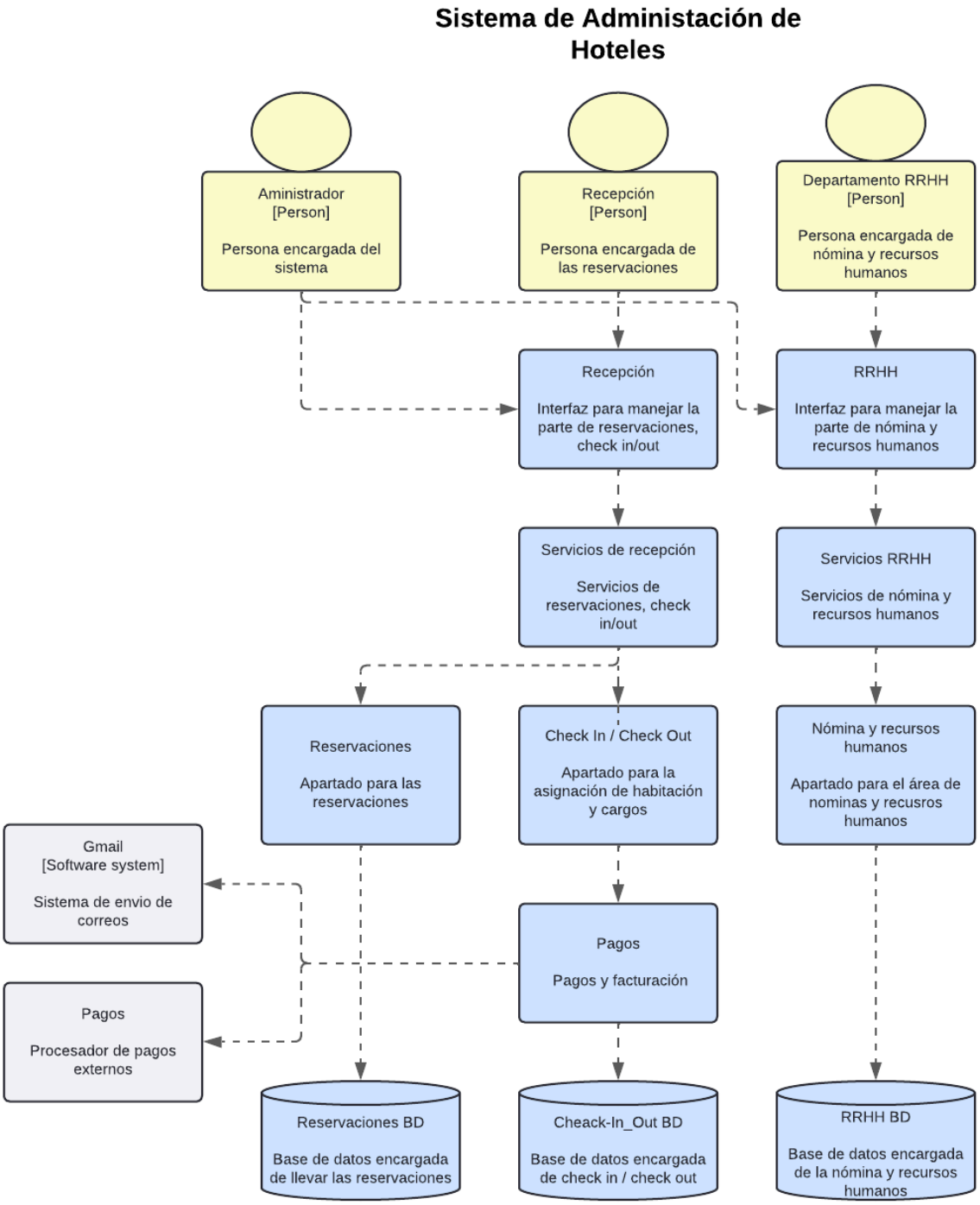
FECHA	TEMA	DESCRIPCIÓN
17/02/2025	Phishing	Phishing Awareness Trainning
19/02/2025	Fuerza Bruta	Password Cracking and Brute Force
21/02/2025	Inyección SQL	Web Application Security Testing: SQL Inyection
23/02/2025	Ransomware	Ransomware Prevention and Protection

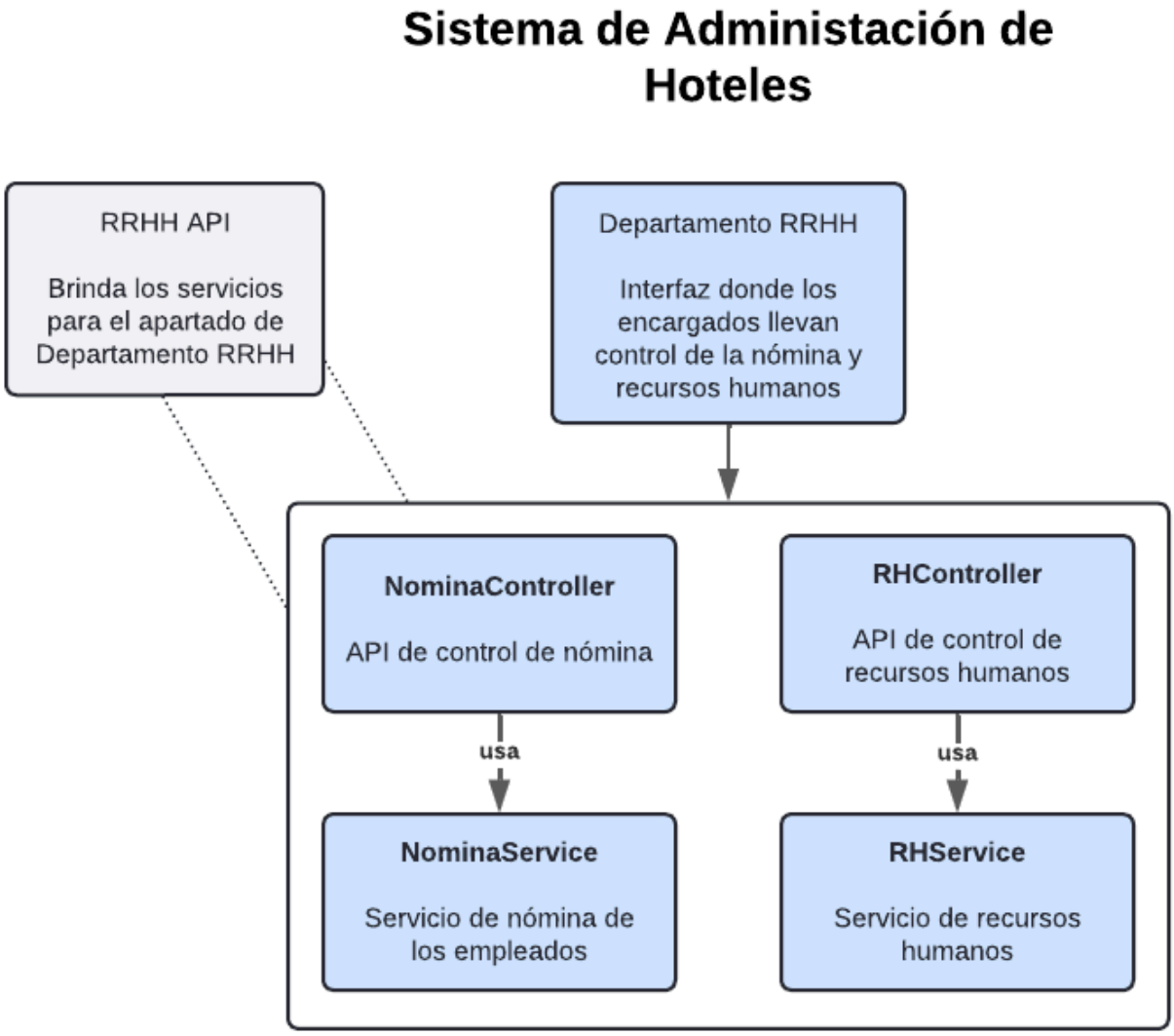
2. Requerimientos funcionales que tendrán impacto en aspectos de seguridad de la aplicación

Requerimientos Funcionales	Nombre de Requisito	Descripción
RNF3	Acceso seguro	El sistema deberá implementar autenticación multifactor para el acceso de usuarios administrativos en todas las sucursales.
RF7	Control de Roles y Permisos	Gestionará el acceso basado en roles (recepcionista, gerente, contador, etc.).
RF16	Integración con Pasarelas de Pago	Permitirá pagos en línea para reservas y cargos adicionales.

3. Diagramas de arquitecturas seguras




Sistema de Administación de Hoteles
Aministrador [Person]
Persona encargada del sistema
Recepción [Person]
Persona encargada de las reservaciones
Departamento RRHH [Person]
Persona encargada de nómina y recursos humanos
Recepción
Interfaz para manejar la parte de reservaciones, check in/out
RRHH
Interfaz para manejar la parte de nómina y recursos humanos
Servicios de recepción
Servicios de reservaciones, check in/out
Servicios RRHH
Servicios de nómina y recursos humanos
Reservaciones
Apartado para las reservaciones
Check In / Check Out
Apartado para la asignación de habitación y cargos
Nómina y recursos humanos
Apartado para el área de nominas y recusros humanos
Gmail [Software system]
Sistema de envio de correos
Pagos
Pagos y facturación
Pagos
Procesador de pagos externos
Reservaciones BD
Base de datos encargada de llevar las reservaciones
Cheack-In_Out BD
Base de datos encargada de check in / check out
RRHH BD
Base de datos encargada de la nómina y recursos humanos



4. Aplicación del enfoque de mínimo privilegio y la reducción de áreas de ataques

1. RNF3: Acceso Seguro (Autenticación Multifactor para Usuarios Administrativos)

Mínimo Privilegio:

- Autenticación multifactor (MFA) asegura que solo usuarios autenticados correctamente puedan acceder a las funciones administrativas. Sin embargo, se debe aplicar el principio de mínimo privilegio otorgando a cada usuario solo los permisos necesarios para realizar su trabajo. Por ejemplo, un administrador de sucursal no debe tener acceso a configuraciones globales o a los datos financieros de la cadena de hoteles a menos que sea estrictamente necesario.

- Gestión de acceso granular: Los privilegios de acceso deben ser estrictamente controlados. Por ejemplo, si un administrador de una sucursal solo necesita gestionar reservas y asignación de habitaciones, no debería tener acceso al módulo de contabilidad ni a los datos de pago de los clientes.

Reducción de Áreas de Ataques:

- Segregación de funciones: Implementar MFA reduce el riesgo de que un atacante pueda tomar control del sistema a través de una sola capa de autenticación. La segregación de funciones, es decir, restringir el acceso a funciones críticas solo a usuarios que realmente las necesiten, también limita la superficie de ataque, dificultando que un atacante consiga acceso a áreas sensibles.
- Auditoría continua: Se deben registrar y auditar todos los accesos y actividades de usuarios administrativos. Esto facilita detectar accesos no autorizados y permite realizar investigaciones en caso de brechas de seguridad.

2. RF7: Control de Roles y Permisos (Acceso Basado en Roles - RBAC)

Mínimo Privilegio:

- El modelo de Control de Acceso Basado en Roles (RBAC) debe garantizar que los usuarios solo puedan acceder a las funcionalidades específicas para las que tienen permisos. Por ejemplo, un recepcionista solo debería poder acceder a la gestión de reservas y check-in/check-out, pero no a la gestión de nómina o la administración de inventarios.
- Asignación de roles adecuados: Debe asegurarse que los roles se asignen de acuerdo con las responsabilidades del personal. Los empleados deben tener solo los permisos necesarios para realizar su trabajo, sin privilegios innecesarios que puedan ser explotados.

Reducción de Áreas de Ataques:

- Acceso restringido a módulos sensibles: Limitar los permisos de acceso al mínimo necesario reduce el número de puntos potenciales de entrada para los atacantes. Si un atacante compromete una cuenta de un empleado con privilegios limitados, su capacidad para acceder a áreas sensibles será reducida.
- Principio de separación de deberes: Se debe garantizar que los roles estén diseñados de manera que las tareas críticas estén separadas y no se concentren en un solo rol. Esto dificulta que un solo atacante comprometa el sistema de manera total, ya que necesitaría acceso a múltiples cuentas para completar un ataque exitoso.

3. RF16: Integración con Pasarelas de Pago (Pagos en Línea para Reservas y Cargos Adicionales)

Mínimo Privilegio:

- Acceso restringido a datos de pago: Solo los usuarios con roles muy específicos (como el personal de contabilidad o gerentes) deben tener acceso a los detalles de las transacciones de pago, y estos accesos deben ser altamente controlados.
- Restricción de permisos en pasarelas de pago: Las integraciones con pasarelas de pago deben tener acceso solo a las funciones necesarias para procesar pagos. El acceso a información bancaria o personal de los clientes debe ser mínimo y protegido con cifrado fuerte.

Reducción de Áreas de Ataques:

- Aislamiento de sistemas de pago: Aislar el sistema de pago de otros componentes del sistema de gestión hotelera reduce las áreas de ataque. Si un atacante compromete una parte del sistema (por ejemplo, el sistema de reservas), el sistema de pagos debería estar aislado y no afectado.
- Cifrado de datos sensibles: Los datos de pago deben ser cifrados tanto en tránsito (usando TLS/SSL) como en reposo. Además, solo los sistemas necesarios deben tener acceso a las claves de cifrado, siguiendo el principio de mínimo privilegio.
- Monitoreo y validación continua: Integrar un sistema de monitoreo y validación de transacciones para detectar comportamientos anómalos en tiempo real. Esto ayuda a identificar ataques, como intentos de fraude en los pagos, antes de que puedan tener un impacto mayor.

5. Componentes críticos para la seguridad como parte de la etapa de diseño

1. Autenticación y Autorización (Identity & Access Management - IAM)

- Implementación de un sistema de autenticación robusto (OAuth 2.0, OpenID Connect) para garantizar que solo usuarios autorizados accedan al sistema.
- Uso de control de acceso basado en roles (RBAC) o basado en atributos (ABAC) para definir los permisos adecuados según las funciones del usuario.
- Integración con proveedores de identidad (IdP) para una autenticación centralizada y segura, como Active Directory, Okta o Auth0.

2. Cifrado y Protección de Datos

- Cifrado de datos en tránsito (TLS/SSL) para proteger la comunicación entre microservicios y con los usuarios finales.
- Cifrado de datos en reposo (AES-256) en bases de datos y almacenamiento para prevenir accesos no autorizados.

- Gestión segura de claves mediante herramientas como AWS KMS, HashiCorp Vault o Azure Key Vault.

3. Monitorización y Detección de Amenazas

- Implementación de un sistema de monitoreo en tiempo real para detectar accesos sospechosos y comportamientos anómalos en el sistema.
- Uso de registros de auditoría centralizados para rastrear actividades y detectar posibles brechas de seguridad.
- Integración con soluciones de detección y respuesta a amenazas (SIEM) como Splunk, ELK Stack o AWS GuardDuty para identificar y mitigar riesgos de seguridad.

Estos componentes son esenciales para garantizar la seguridad de la plataforma, proteger la información sensible y minimizar vulnerabilidades dentro del ecosistema de la cadena hotelera.

6. Definición de los roles, permisos y privilegios de la aplicación

1. Roles Definidos en la Aplicación

Cada usuario del sistema pertenecerá a uno de los siguientes roles, con privilegios específicos:

A. Administrador General

📌 **Descripción: Usuario con el nivel más alto de acceso en la plataforma, perteneciente a la matriz en la Ciudad de México.**
🔹 **Permisos:**

- **Configurar parámetros globales del sistema.**
- **Administrar la base de datos de empleados y sucursales.**
- **Gestionar la asignación de roles y permisos a usuarios.**
- **Supervisar reportes de operación y auditoría.**
- **Control total sobre todos los módulos.**

B. Gerente de Sucursal

📌 **Descripción: Responsable de la operación de una sucursal específica.**
🔹 **Permisos:**

- **Gestionar reservas, check-in y check-out.**
- **Acceder a reportes operativos y financieros de su sucursal.**
- **Administrar la nómina y recursos humanos dentro de la sucursal.**
- **Autorizar cambios en asignación de habitaciones.**

C. Recepcionista

📌 **Descripción: Encargado del proceso de atención al huésped en recepción.**
🔹 **Permisos:**

- **Gestionar check-in y check-out de huéspedes.**
- **Ver disponibilidad y asignar habitaciones.**
- **Modificar reservas dentro de los parámetros definidos.**
- **Emitir facturas y gestionar pagos.**

D. Contador

📌 **Descripción: Responsable del manejo financiero de la sucursal.**
🔹 **Permisos:**

- **Acceder a reportes financieros y contables.**
- **Procesar pagos, facturación y devoluciones.**
- **Control de impuestos y cumplimiento fiscal.**

E. Recursos Humanos

📌 **Descripción: Encargado de la administración del talento humano en cada sucursal.**
🔹 **Permisos:**

- **Gestionar nómina y empleados.**
- **Administrar contratación y despidos.**
- **Acceder a reportes de desempeño y asistencia.**

F. Usuario Cliente (Huésped)

📌 **Descripción: Cliente que utiliza la aplicación para realizar reservaciones.**
🔹 **Permisos:**

- **Consultar disponibilidad y realizar reservas.**
- **Modificar o cancelar reservas dentro de los términos permitidos.**
- **Realizar pagos en línea y recibir confirmaciones.**

Módulo del Sistema	Administrador General	Gerente de Sucursal	Recepcionista	Contador	Recursos Humanos	Huésped
Gestión de Usuarios	✅ Crear, modificar, eliminar	✅ Gestionar empleados de sucursal	❌	❌	❌	❌
Gestión de Reservas	✅	✅	✅	❌	❌	✅ Solo propias
Check-In / Check-Out	✅	✅	✅	❌	❌	❌
Contabilidad y Facturación	✅	✅	❌	✅	❌	✅ Solo pagos
Nómina y RRHH	✅	✅	❌	❌	✅	❌
Reportes Generales	✅	✅ Solo de sucursal	❌	✅	✅	❌

✅ = Acceso permitido
❌ = Acceso restringido

Bibliografía

- **Material visto en classroom**

- **Ortega Candel, J. M. (2020). *Desarrollo seguro en ingeniería del software* (1ª ed.). MARCOMBO, S. L.**