

UNIVERSIDAD TECNOLÓGICA DE XICOTEPEC DE JUÁREZ PUEBLA

INGENIERÍA EN DESARROLLO Y GESTIÓN DE SOFTWARE
CUATRIMESTRE ENERO-ABRIL DE 2024



**DOCUMENTACION DEL PROYECTO INTEGRADOR MÓDULO:
RECURSOS HUMANOS**

ELABORÓ:

AMÉRICA YAELY ESTUDILLO LICONA M-200525
JONATHAN ENRIQUE IBARRA CANALES M-210128
JESÚS RÍOS GÓMEZ M-200995

PLAN DE SEGURIDAD DE LA BD DEL MODULO DE RECURSOS HUMANOS

Introducción

En el entorno altamente sensible y regulado de un hospital, la gestión de los recursos humanos es fundamental para el funcionamiento eficiente y efectivo de la institución. El módulo de Recursos Humanos no solo almacena información vital sobre los empleados, como datos personales, historiales laborales y registros de capacitación, sino que también juega un papel crucial en la toma de decisiones estratégicas y operativas del hospital.

La protección de la información confidencial y sensible del personal es una prioridad absoluta para garantizar la privacidad, integridad y disponibilidad de los datos. La seguridad de estos datos no solo es esencial para proteger los derechos y la privacidad de los empleados, sino que también es un requisito legal y regulatorio, ya que los hospitales están sujetos a estrictas normativas de protección de datos, como la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA, por sus siglas en inglés) en los Estados Unidos o la Ley Orgánica de Protección de Datos Personales (LOPD) en España.

Este plan de seguridad está diseñado para proporcionar una guía integral para proteger la información del personal almacenada en el módulo de Recursos Humanos del hospital. Se enfoca en establecer roles, usuarios y privilegios adecuados, así como en brindar recomendaciones prácticas para el respaldo de la base de datos y medidas adicionales de seguridad para mitigar posibles riesgos y amenazas.

La implementación efectiva de este plan no solo garantizará el cumplimiento de las regulaciones de protección de datos, sino que también fortalecerá la confianza de los empleados en la seguridad de su información personal y contribuirá a la reputación y credibilidad del hospital como institución comprometida con la protección de la privacidad y la seguridad de sus empleados.

Roles, Usuarios y Privilegios

1. Administrador de Recursos Humanos:

- Responsable de la gestión general del sistema de Recursos Humanos.
- Tiene acceso completo al módulo de Recursos Humanos.
- Puede agregar, editar y eliminar registros de empleados.
- Tiene el privilegio de asignar roles y privilegios a otros usuarios del sistema.

2. Gestor de Personal

- Encargado de las operaciones diarias del módulo de Recursos Humanos.
- Puede ver y actualizar la información de los empleados.
- Tiene permisos limitados para modificar ciertos datos sensibles, como salarios y evaluaciones de desempeño.

3. Empleado

- Tiene acceso limitado para ver y actualizar su propia información personal.
- Puede acceder a documentos como su contrato laboral, formularios de permisos y registros de vacaciones.

Recomendaciones para el Respaldo de la Base de Datos:

1. Realizar copias de seguridad regulares de la base de datos del módulo de Recursos Humanos, preferiblemente diariamente o semanalmente, dependiendo de la criticidad de los datos.
2. Almacenar las copias de seguridad en ubicaciones seguras y fuera del sitio para proteger contra pérdidas de datos debido a desastres naturales o incidentes de seguridad.

3. Probar regularmente la restauración de las copias de seguridad para asegurarse de que sean válidas y se puedan recuperar en caso de emergencia.
4. Implementar medidas de seguridad adicionales, como cifrado de datos, para proteger las copias de seguridad contra accesos no autorizados.

Recomendaciones Adicionales

1. Capacitar al personal del departamento de Recursos Humanos sobre las políticas de seguridad de la información y las mejores prácticas para proteger los datos confidenciales.
2. Implementar controles de acceso basados en roles para garantizar que cada usuario tenga acceso solo a la información necesaria para realizar sus funciones.
3. Mantener el software del sistema de Recursos Humanos actualizado con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.
4. Realizar auditorías periódicas de seguridad para identificar posibles riesgos y mejorar continuamente las medidas de seguridad.