



UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL SAN RAFAEL
MENDOZA

Tecnicatura Superior en Programación

LEGISLACIÓN

Trabajo Práctico Individual N°2
“Normas Internas y la ISO 25010”

ALUMNA

Ríos Garín, Ana Paula (11.212)

GRUPO

Carpinchos Programando

PROFESORES

Lic. Sánchez, Miguel

Ing. Giordanini, Osvaldo

Fecha Límite de Entrega: 18/09

2025

ÍNDICE

CONSIGNAS	1
INTRODUCCIÓN	2
RESUMEN	3
RESPUESTAS	4
1. Norma Interna: Gestión de Claves de ...	4
Objetivo	4
Alcance	4
Procedimientos Clave	4
Relación con la ISO 25010	4
Responsables	4
2. Norma Interna: Copias de Resguardo ...	4
Objetivo	4
Alcance	4
Procedimientos Clave	4
Relación con la ISO 25010	5
Responsables	5
3. Norma Interna: Ambientes de Trabajo ...	5
Objetivo	5
Alcance	5
Procedimientos Clave	5
Relación con la ISO 25010	5
Responsables	5
Conclusión sobre la Elección y Aplicaciones ...	5
CONCLUSIÓN	7
BIBLIOGRAFÍA	8

CONSIGNAS

- Adoptar al menos tres normas internas (grilla de normativas modelos), para cumplir con la preparatoria de certificar garantía con ISO 25010. Además, incluir una breve y sencilla conclusión sobre el motivo que origina la elección y aplicación de dichas normas.

PRESENTAR TRABAJO EN TIEMPO Y FORMA CONVENIDA CON:

Su debida y adecuada documentación. (papeles de trabajo profesional).

- Resumen.
- Antecedentes.
- Comentarios.
- Posibles soluciones profesionales.
- Normativas relacionadas (ejemplos usados).
- Apellido y nombre, matrícula individual.

INTRODUCCIÓN

La norma **ISO 25010** es un estándar internacional que define un modelo de calidad para productos de software, estableciendo características y subcaracterísticas que permiten evaluar y garantizar la calidad tanto del producto como de su uso. Preparar una organización para la certificación bajo este estándar requiere la implementación de normas internas que aseguren el cumplimiento de estos criterios. Este trabajo presenta la adopción de tres normas internas basadas en el marco normativo proporcionado, las cuales se alinean directamente con los requisitos de la ISO 25010, específicamente en las características de **Seguridad, Mantenibilidad y Capacidad de Interacción**. Además, se incluye una conclusión que justifica la selección de estas normas y su contribución a la preparación para la certificación.

RESUMEN

Este trabajo tiene como objetivo seleccionar y adaptar tres normas internas que faciliten la preparación para la certificación bajo la norma ISO 25010. Las normas elegidas son:

1. **Gestión de Claves de Acceso** (basada en NOR223 y NOR224), que aborda la seguridad y la confidencialidad.
2. **Copias de Resguardo** (basada en NOR231), que garantiza la mantenibilidad y la recuperabilidad.
3. **Ambientes de Trabajo y Funciones** (basada en NOR232), que asegura la capacidad de interacción y la integridad del software.

Cada norma se describe detalladamente, incluyendo su objetivo, alcance, procedimientos clave y relación con la ISO 25010. La conclusión destaca cómo estas normas contribuyen colectivamente a cumplir con los requisitos del estándar internacional y a mejorar la calidad del software.

RESPUESTAS

Para preparar la organización para la certificación bajo el estándar **ISO 25010**, que evalúa la calidad del producto software y la calidad en uso, es fundamental implementar normas internas que aseguren el cumplimiento de sus características y subcaracterísticas. A continuación, se seleccionan y adaptan tres normas internas clave, basadas en el marco normativo provisto, que directamente apoyan los requisitos de la ISO 25010, particularmente en las características de **Seguridad, Mantenibilidad y Capacidad de Interacción**.

1. NORMA INTERNA: GESTIÓN DE CLAVES DE ACCESO (BASADA EN NOR223 Y NOR224)

OBJETIVO

Establecer los requisitos mínimos para la creación, gestión y protección de claves de acceso (contraseñas) para garantizar la autenticación segura de usuarios y la confidencialidad de los datos.

ALCANCE

Aplica a todos los clientes internos y externos que accedan a sistemas computarizados de la organización.

PROCEDIMIENTOS CLAVE

- Asignar una identificación única por usuario.
- Utilizar contraseñas con longitud mínima de 6 caracteres, combinando caracteres alfanuméricos.
- Encriptar y almacenar contraseñas en archivos protegidos.
- Obligar al cambio periódico de contraseñas (cada 30 días) y evitar la reutilización de las últimas 5.
- Bloquear accesos tras múltiples intentos fallidos.
- Registrar eventos de acceso para auditoría.

RELACIÓN CON ISO 25010

Esta norma contribuye directamente a la **Seguridad (ISO 25010)**, específicamente a las subcaracterísticas de:

- **Confidencialidad:** Protección de datos contra accesos no autorizados.
- **Autenticidad:** Verificación de la identidad de los usuarios.
- **Responsabilidad:** Trazabilidad de acciones mediante registros de acceso.

RESPONSABLES

Administrador de seguridad, clientes de los sistemas, y Auditoría de Sistemas.

2. NORMA INTERNA: COPIAS DE RESGUARDO (BASADA EN NOR231)

OBJETIVO

Definir estrategias para la generación, almacenamiento y recuperación de copias de respaldo (backup) que aseguren la integridad y disponibilidad de los datos.

ALCANCE

Aplica a todas las áreas de servicios informáticos y plataformas de procesamiento.

PROCEDIMIENTOS CLAVE

- Realizar copias totales semanales, progresivas diarias e incrementales diarias.

- Almacenar dos copias: una dentro y otra fuera del edificio, en lugares ignífugos.
- Rotular soportes con información detallada (fecha, sistema, operador, etc.).
- Registrar movimientos de soportes y mantener un inventario actualizado.
- Probar periódicamente los mecanismos de restauración.

RELACIÓN CON ISO 25010

Esta norma aborda la **Mantenibilidad (ISO 25010)**, en particular:

- **Analizabilidad:** Facilidad para diagnosticar fallos mediante registros de backup.
- **Modificabilidad:** Capacidad de restaurar sistemas a estados anteriores.
- **Recuperabilidad:** Garantía de disponibilidad tras incidentes.

RESPONSABLES

Responsable de datos, administrador de seguridad, explotación y biblioteca.

3. NORMA INTERNA: AMBIENTES DE TRABAJO Y FUNCIONES (BASADA EN NOR232)

OBJETIVO

Separar física y lógicamente los ambientes de desarrollo, prueba y producción para prevenir accesos no autorizados y garantizar la integridad del software.

ALCANCE

Aplica a clientes internos/externos que interactúen con ambientes de producción y/o desarrollo.

PROCEDIMIENTOS CLAVE

- Implementar bibliotecas segregadas: software de base, desarrollo, control y producción.
- Restringir acceso al ambiente de producción para personal de desarrollo.
- Requerir autorización escrita y monitoreo para intervenciones de soporte técnico.
- Mantener programas fuentes en bibliotecas seguras con acceso restringido.

RELACIÓN CON ISO 25010

Esta norma se alinea con la **Capacidad de Interacción (ISO 25010)** y la **Mantenibilidad:**

- **Protección contra errores:** Evita modificaciones accidentales o no autorizadas.
- **Modularidad:** Organización clara de componentes software.
- **Operabilidad:** Facilita el uso correcto por roles autorizados.

RESPONSABLES

Responsable de servicios informáticos, administrador de seguridad, y Auditoría de Sistemas.

CONCLUSIÓN SOBRE LA ELECCIÓN Y APLICACIÓN DE LAS NORMAS

La selección de estas tres normas internas—**Gestión de Claves de Acceso, Copias de Resguardo y Ambientes de Trabajo y Funciones**—se fundamenta en su directa contribución a los requisitos de seguridad, mantenibilidad y capacidad de interacción exigidos por la **ISO 25010**.

- **Gestión de Claves de Acceso** asegura la autenticación y confidencialidad, críticas para la seguridad del producto.

- **Copias de Resguardo** garantiza la disponibilidad y recuperabilidad, esenciales para la mantenibilidad y continuidad operativa.
- **Ambientes de Trabajo y Funciones** previene errores y accesos no autorizados, apoyando la capacidad de interacción y la integridad del software.

Estas normas no solo preparan a la organización para la certificación ISO 25010, sino que también establecen un marco de control proactivo que reduce riesgos, mejora la calidad del software y aumenta la confianza de los stakeholders. Su implementación demuestra un compromiso con la excelencia en la gestión de la calidad del software.

CONCLUSIÓN

La selección de estas tres normas internas—**Gestión de Claves de Acceso, Copias de Resguardo y Ambientes de Trabajo y Funciones**—se fundamenta en su directa contribución a los requisitos de seguridad, mantenibilidad y capacidad de interacción exigidos por la **ISO 25010**.

- **Gestión de Claves de Acceso** asegura la autenticación y confidencialidad, críticas para la seguridad del producto.
- **Copias de Resguardo** garantiza la disponibilidad y recuperabilidad, esenciales para la mantenibilidad y continuidad operativa.
- **Ambientes de Trabajo y Funciones** previene errores y accesos no autorizados, apoyando la capacidad de interacción y la integridad del software.

Estas normas no solo preparan a la organización para la certificación ISO 25010, sino que también establecen un marco de control proactivo que reduce riesgos, mejora la calidad del software y aumenta la confianza de los stakeholders. Su implementación demuestra un compromiso con la excelencia en la gestión de la calidad del software.



BIBLIOGRAFÍA

1. ISO 25010:2011 - Systems and software engineering.
 - <https://www.iso.org/standard/35733.html>
2. ISO 25010.
 - <https://iso25000.com/index.php/en/iso-25000-standards/iso-25010>
3. Understanding ISO 25010.
 - <https://www.qmii.com/understanding-iso-25010-navigating-the-seas-of-software-quality/>
4. An Exploration of the ISO 25010 Software Quality Model.
 - <https://blog.codacy.com/iso-25010-software-quality-model>