
**Política de desarrollo seguro**

**Propietario de la política: VICTOR ACOSTA LOPEZ**

**Fecha de entrada en vigencia: 09/04/2024**

**Objetivo**

Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida del desarrollo de aplicaciones y sistemas de información.

**Alcance**

Todas las aplicaciones y sistemas de información de D3M3NT SA DE CV que son críticos para el negocio o que procesan, almacenan o transmiten datos confidenciales. Esta política se aplica a

todos los ingenieros y desarrolladores internos y externos de *software* e infraestructura de D3M3NT SA DE CV.

**Política**

Esta política describe las reglas para la adquisición y el desarrollo de *software* y los sistemas que se aplicarán a los desarrollos dentro de la organización de D3M3NT SA DE CV.

**Procedimientos de control de cambios en el sistema**

Los cambios en los sistemas dentro del ciclo de vida de desarrollo se controlarán mediante el uso de procedimientos formales de control de cambios. Los procedimientos y requisitos de control de cambios se describen en la Política de Seguridad de las Operaciones de D3M3NT SA DE CV.

Los cambios significativos en el código deben ser revisados y aprobados por GERENTE TI antes de fusionarse en cualquier rama de producción de acuerdo con el Proceso de Revisión que se determine de acuerdo al proyecto ejecutado, deberá estar registrado en monday.com

Los procedimientos de control de cambios garantizarán que no sea una sola persona sin aprobación ni supervisión quién realice el desarrollo, las pruebas y la implementación de cambios.

**Control de versiones de *software***

Todo el *software* de D3M3NT SA DE CV se controla y sincroniza entre los colaboradores (desarrolladores). El acceso al repositorio central se restringe según la función del empleado. Todo el código se escribe, se prueba y guarda en un depósito local antes de sincronizarse con el depósito de origen.

**Revisión técnica de aplicaciones después de cambios en la plataforma operativa**

Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio se revisarán y se probarán para garantizar que no haya un impacto adverso en las operaciones o la seguridad de la organización.

**Restricciones en los cambios a los paquetes de software**

No se aconsejarán las modificaciones a los paquetes de aplicaciones comerciales de terceros, se limitará a los cambios necesarios y todos los cambios deberán controlarse estrictamente.

**Principios de ingeniería de sistemas seguros**

Se establecerán, documentarán, mantendrán y aplicarán los principios de ingeniería de sistemas seguros a cualquier intento de implementación de sistemas de información.

Como mínimo, se aplicarán los siguientes principios de seguridad por diseño y privacidad por diseño:

Principios de seguridad por diseño:

1. Minimizar el área de superficie de ataque
2. Establecer valores predeterminados seguros
3. El principio del mínimo privilegio
4. El principio de defensa en profundidad
5. Falla de forma segura
6. No confíe en los servicios
7. Separación de tareas
8. Evitar la seguridad por oscuridad

9. Mantenga la seguridad simple
10. Solucionar los problemas de seguridad correctamente

Principios de privacidad por diseño:

1. Proactivo no reactivo; preventivo no correctivo
2. La privacidad como configuración predeterminada
3. Privacidad integrada en el diseño
4. Funcionalidad completa: suma positiva, no suma cero
5. Seguridad integral: protección completa del ciclo de vida
6. Visibilidad y transparencia: mantener abiertas
7. Respeto por la privacidad del usuario: mantenerlo centrado en el usuario

Los documentos de ingeniería y las referencias técnicas se pueden encontrar en https://github.com/vidmente

Se espera que los desarrolladores de *software* cumplan con los estándares de codificación de D3M3NT SA DE CV durante todo el ciclo de desarrollo, incluidos los estándares de calidad, comentarios y seguridad.

**Entorno de desarrollo seguro**

D3M3NT SA DE CV establecerá y protegerá adecuadamente los entornos para los intentos de desarrollo e integración de sistemas que abarquen todo el ciclo de vida de desarrollo del sistema. Los siguientes entornos se segregarán lógica o físicamente:

- Producción
- Prueba / Etapas
- Desarrollo

**Desarrollo externalizado**

D3M3NT SA DE CV supervisará y controlará la actividad del desarrollo de sistemas subcontratados. El desarrollo subcontratado deberá cumplir con todos los estándares y políticas de D3M3NT SA DE CV.

**Pruebas de seguridad del sistema**

Las pruebas de la funcionalidad de seguridad se realizarán en períodos definidos durante el ciclo de vida del desarrollo. No se implementará ningún código en los sistemas de producción de D3M3NT SA DE CV sin resultados de prueba documentados y exitosos y la evidencia de las actividades de refuerzo de seguridad.

**Administración de vulnerabilidad de las aplicaciones**

El código de aplicación se debe escanear antes de la implementación. Los parches para abordar las vulnerabilidades de las aplicaciones que afectan sustancialmente la seguridad deben implementarse dentro de los 90 días posteriores a la detección.

**Pruebas de aceptación del sistema**

Se establecerán programas de prueba de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.

Antes de desplegar el código, debe completarse una lista de verificación de lanzamiento que incluya una lista de verificación de todos los planes de prueba que muestren la finalización de todas las pruebas asociadas y la corrección de los problemas identificados.

**Protección de datos de prueba**

Los datos de prueba se seleccionarán cuidadosamente, estarán protegidos y controlados. Los datos confidenciales del cliente se protegerán de acuerdo con todos los contratos y compromisos. Los datos del cliente no se utilizarán para fines de prueba sin el permiso explícito del propietario de los datos y el GERENTE TI.

**Adquisición de sistemas y *software* de terceros**

La adquisición de sistemas y *software* de terceros se realizará de conformidad con los requisitos de la Política de Gestión de Terceros de D3M3NT SA DE CV.

**Capacitación para desarrolladores**

Se proporcionará a los desarrolladores de *software* una capacitación de desarrollo segura y adecuada a su función, al menos, una vez al año. El contenido de la capacitación estará determinado por la administración, pero abordará la prevención de ataques y vulnerabilidades comunes a las aplicaciones web. Las siguientes amenazas y vulnerabilidades deben abordarse según corresponda:

- Prevención de ataques de omisión de autorización
- Prevención del uso de identificadores de sesión no seguros
- Prevención de ataques de inyección
- Prevención de ataques de secuencias de comandos entre sitios
- Prevención de ataques de falsificación de solicitudes cruzadas
- Prevención del uso de bibliotecas vulnerables

**Excepciones**

Las solicitudes de excepción a esta Política deben enviarse al GERENTE TI para su aprobación.

**Infracciones y cumplimiento**

Todas las infracciones conocidas de esta política deben notificarse al GERENTE TI.. Las infracciones de esta política pueden dar lugar a la cancelación o suspensión inmediata de los privilegios del sistema y de la red o a medidas disciplinarias de conformidad con los procesos de la empresa, incluido el despido.

| Versión | Fecha | Descripción | Autor | Aprobado por |
|---|---|---|---|---|
| 1.1 | 09/04/2024 | AJUSTES POR TRADUCCCION | VICTOR ACOSTA | MARCO VILLANUEVA |
| | | | | |