Política Específica de Seguridad en el Desarrollo Seguro

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo de esta política es garantizar la seguridad de la información como parte integral del ciclo de vida del desarrollo del software que produce DACTA.

Este documento se aplica a todo el alcance del Sistema de Integrado de Gestión (SIG).

Los usuarios de este documento son todos los colaboradores y proveedores involucrados en el desarrollo y Testing de sistemas en DACTA.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO 9001:2015 (Sistema de Gestión de la Calidad).
- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, clausulas 8.4, 8.25, 8.26, 8.27, 8.28, 8.29, 8.30, 8.31.
- Norma ISO 37001:2016 (Sistema de Gestión Anti soborno).
- L-E-SIG-01 Política Integrada del SIG
- L-E-SIG-05 Política Específica de Gestión de Accesos
- S-RRHH-P2-F2 Programa anual de Capacitación
- L-E-SIG-003 Política Específica de Gestión de Base de Datos

3. POLÍTICA ESPECÍFICA

3.1. DE LA POLÍTICA DE DESARROLLO SEGURO

Esta Política de Desarrollo Seguro comprende las reglas para el desarrollo de software y sistemas informáticos dentro de DACTA. Para esto, se establecen los siguientes lineamientos:

1. Se deberán utilizar técnicas de programación seguras tanto para los desarrollos nuevos como en las situaciones de reutilización de códigos donde es posible que no se conozcan las normas que se aplicaron a dicho desarrollo o donde no sean coherentes con las buenas prácticas actuales.
2. Se debe estandarizar el ciclo de vida del desarrollo de software en DACTA, con los objetivos de:
   - Definir claramente las actividades a ejecutarse dentro un proyecto de desarrollo de software.
   - Identificar riesgos y
   - Unificar criterios en la organización para el desarrollo de software.
   - Establecer puntos de control y revisión en todas las etapas del desarrollo.
3. Se deben estandarizar, los criterios de seguridad y calidad, que serán considerados, durante cada fase del proceso de desarrollo de sistemas de información.
4. En caso el desarrollo de algunas aplicaciones se tuviera que realizar por terceros, se deben celebrar contratos, con los proveedores, incluyendo cláusulas, que resguarden de manera taxativa la propiedad intelectual para DACTA y, asimismo aseguren, los requisitos de confidencialidad de la información en el proyecto respectivo.

3.2. DEL ENTORNO DE DESARROLLO SEGURO

El Entorno de desarrollo seguro en DACTA considera los aspectos de seguridad de la información en:

1. El entorno de desarrollo, identificado como el conjunto de procesos y herramientas que se utilizan para desarrollar un código fuente o programa.
2. Todas las etapas del desarrollo del software que desarrolla o produce

DACTA.

3. El ciclo de desarrollo de software, en particular:
   - Seguridad en la metodología de desarrollo de software.
   - Pautas de codificación segura para cada lenguaje de programación que se utiliza.
4. El establecimiento de puntos de verificación de seguridad dentro de los hitos de los proyectos de desarrollo de software y sistemas.
5. Los repositorios de información asociados a los proyectos de desarrollo de software y sistemas.
6. El manejo del control de versiones de los proyectos de desarrollo de software y sistemas.
7. La capacidad del equipo de desarrollo para:
   - Conocer las condiciones de seguridad de las aplicaciones desarrolladas.
   - Evitar, encontrar y resolver las vulnerabilidades de los desarrollos de software y sistemas.

3.3. PRUEBAS DE SEGURIDAD DEL SISTEMA

1. Toda aplicación, dentro del ciclo de desarrollo debe incluir una etapa de Pruebas. En esta etapa, toda aplicación se someterá a pruebas y verificaciones incluyendo las de seguridad. Para ello se debe contar con programa de actividades detallado, entradas de pruebas y los resultados esperados bajo una variedad de condiciones.
2. Se recomienda, que las pruebas del sistema, incluyan, entre otros aspectos; instalación, volumen, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores, como mínimo.
3. Dentro de lo posible, las pruebas, deben ser realizadas, almacenando criterios y datos de pruebas en archivos, de modo de permitir la verificación rápida y repetitiva.

3.4. PRUEBAS DE APROBACIÓN DEL SISTEMA

1. Las pruebas de aceptación de sistemas, se deberán realizar en un Ambiente de Pruebas y en un Ambiente Beta, de tal forma que permita, garantizar que el sistema no introducirá vulnerabilidades a ningún entorno donde tenga que funcionar. Asimismo, se debe asegurar, que las pruebas sean confiables.
2. Para realizar las pruebas de aceptación de sistemas, se podrán utilizar las herramientas automatizadas disponibles en el mercado, como las herramientas de análisis de códigos o los escáneres de vulnerabilidad y debería verificar la remediación de los defectos relacionados con la seguridad.

3.5. INFORMACIÓN PARA LAS PRUEBAS

1. El cliente, propietario de la información en las Bases de datos, debe ser informado que para las pruebas se utilizará el backup al cierre del último día, previo a la realización de las pruebas.
2. La información de clientes, en las bases de datos que se utilicen en ambientes de Desarrollo y Pruebas de calidad del software debe estar ofuscada. En los casos que técnicamente haya complicaciones para ofuscarla, el Oficial de Seguridad debe autorizar el uso de la información sin la debida ofuscación. La información en ambiente Beta queda exonerada de esta condición.
3. El acceso a las bases de datos debe ser accedida únicamente por personal previamente identificado y que cuente con el acuerdo de confidencialidad actualizado y firmado.

3.6. SEPARACIÓN DE ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN

1. Los ambientes de desarrollo, prueba y producción, estarán separados

preferentemente en forma física dentro de la infraestructura de computación de DACTA.

2. Todos los desarrollos deberán considerar al menos los siguientes ambientes:
   - Ambiente de Desarrollo
   - Ambiente de Pruebas
   - Ambiente Beta
   - Ambiente de Producción

3.7. DEL CONTROL DE VERSIONES

1. Es responsabilidad de todo el equipo de desarrollo, con su líder a la cabeza, de definir, mantener actualizado permanentemente y de difundir un adecuado sistema de control de versiones de todas las aplicaciones que se desarrollen.

2. Todo software desarrollado nuevo, debe contar con un código de versión identificable y leíble por todo el equipo DEVOPS, tanto en el back end como en el front end. Las modificaciones a objetos de una versión en productivo también conllevarán a una actualización del código de versión necesaria y suficiente para un adecuado manejo de las aplicaciones frente al cliente.

3. Cada nueva versión que los desarrolladores lancen a Testing debe incluir una documentación como mínimo:
   a) Código de versión
   b) Relación de cambios incluidos
   c) Ambiente o plataforma donde se ejecutará
   d) Requisitos y/o requerimientos a cumplir para el Testing
   e) Requisitos y/o requerimientos a cumplir para la puesta en productivo

3.8. DE LOS REQUERIMIENTOS DE CLIENTES

1. Todo nuevo proyecto de desarrollo de software o modificación de software debe trabajarse exclusivamente en los ambientes de desarrollo de la empresa. [9001-27001]
2. Todo desarrollo de software debe efectuarse atendiendo estrictamente a las políticas de calidad, de seguridad de la información y a las normas vigentes sean estas internas o externas. [9001-27001-37001]
3. Por tanto, cualquier propuesta de desarrollar aplicaciones cuyo funcionamiento transgreda la ley será rechazada de inmediato y reportada en el canal de denuncias [37001].
4. Para dar inicio a un nuevo desarrollo se debe contar con la documentación necesaria y suficiente aprobada por el cliente y la Gerencia de Proyectos. El tipo de documentación y su contenido será definido en coordinación con la Gerencia de Proyectos.
5. Todo desarrollo culminado debe incluir la documentación técnica necesaria y suficiente para que personal de las otras áreas, integrantes de DEVOPS, puedan manipular los objetos componentes de ese desarrollo de manera autónoma y autosuficiente durante las siguientes etapas al proceso del desarrollo.

3.9. DE LA PLANIFICACIÓN DE RECURSOS DE DESARROLLO

1. Todos los recursos asignados, por la empresa, para la ejecución de los desarrollos de software deben ser administrados atendiendo los criterios de calidad, legalidad, seguridad de la información, de eficiencia y de estricto cumplimiento de la metodología de DEVOPS.
2. Será responsabilidad directa del líder de desarrollo;
   a) Asegurarse que el personal a su cargo cumpla con todos los lineamientos establecidos para atender la metodología de DEVOPS.

b) Definir los objetivos semanales, quincenales y mensuales del equipo de desarrollo en coordinación con la Gerencia de Proyectos y con el personal a su cargo.
c) Organizar y elaborar los planes de asignación de recursos para la ejecución de los proyectos de desarrollo, atendiendo a los criterios de oportunidad, prioridad y del logro de objetivos de la empresa.
d) Evaluar permanente los avances y logros de cada integrante del equipo de desarrollo, midiendo la desviación de los tiempos programados vs. los realizados y el logro de objetivos, para lo cual debe generar el entorno necesario para que el personal a su cargo actualice diariamente sus avances.

3.10. DE LA CAPACITACIÓN DEL PERSONAL DE DESARROLLO

1. El equipo de desarrollo, con su líder a la cabeza, deberá actualizarse permanentemente en el entendimiento de las nuevas tecnologías enfocadas al desarrollo de software y propiciar su incorporación dentro de los desarrollos que se realicen dentro de la empresa sustentando los beneficios a obtener.
2. Todo personal nuevo debe pasar por un proceso de inducción necesario y suficiente para que se empape de las actividades que debe realizar.
3. Será responsabilidad directa del líder de Desarrollo:
   a) Evaluar el rendimiento de cada integrante del equipo de desarrolladores asignado y bajo su dirección.
   b) Determinar la conveniencia de capacitar a un integrante del equipo o a todo el equipo de desarrolladores en temas que propicien un mejor rendimiento de cada integrante o permitan un salto cualitativo y/o cuantitativo en los resultados del proceso de Desarrollo.
   c) Elaborar un plan de capacitación del personal a su cargo en función de los objetivos trazados por la empresa y de los cambios de carácter metodológico, técnico que se vayan ejecutando al interior del proceso de Desarrollo.
   d) Gestionar los recursos necesarios para la realización de capacitaciones.

4. Todo proceso de inducción o de capacitación conllevará a:
   a) Una programación previa especificando el objetivo de la capacitación, temario o contenido de la capacitación, fecha de inicio, duración, horarios, participantes.
   b) La asignación de recursos técnicos para que el o los capacitados reciban una instrucción vivencial en los temas programados.
   c) Una evaluación teórica práctica obligatoria al (o los) participante(s) y con puntuación. El resultado de esta evaluación debe ser reportado a Recursos Humanos.
   d) Asistencia obligatoria del personal incluido en la relación.

3.11. DE LOS ESTÁNDARES DE PROGRAMACIÓN

1. El equipo de desarrollo, con su líder a la cabeza, será responsable de propiciar la adopción o impulsar el desarrollo y posterior implementación de:
   a. La aplicación de buenas prácticas durante todo el ciclo de desarrollo de software.
   b. Estándares que aseguren un trabajo uniforme entre todos los desarrolladores.
   c. Metodologías y/o técnicas que aseguren un eficiente y efectivo proceso de desarrollo de software.
   d. Controles que aseguren la detección oportuna de cualquier desviación del objetivo trazado.
2. El cumplimiento de las directivas incluidas en el Manual de estándares tendrá el carácter de obligatorio para todo el personal de desarrollo.

3. El equipo de desarrollo, con su líder a la cabeza, será responsable de incluir en todo desarrollo, desde su inicio, los principios de Desarrollo seguro de software siendo esta directiva de cumplimiento obligatorio.

3.12. DE LA SEGURIDAD DE LA INFORMACIÓN Y CUMPLIMIENTO DE NORMAS.

1. El personal de desarrollo está prohibido acceder a los datos sensibles de los ambientes en producción. [27001].
2. Los programadores están prohibidos de actualizar información directamente en la base de datos de producción. En los casos que sea muy necesario lo debe autorizar formalmente el coordinador del área.
3. La inhabilitación de objetos de Bases de datos en producción está prohibida. De ser necesaria esta acción se debe llevar un control documentado de cada vez que se requiera efectuar la inhabilitación. El registro se debe hacer antes de ejecutar la acción y una vez culminada la actividad que demandó esta inhabilitación se debe registrar la activación.

El incumplimiento de la presente Política Específica será considera falta grave, siendo el colaborador susceptible de sanción o penalidad. Los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará al Oficial de Seguridad para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, la autoridad competente de DACTA, tomará las medidas disciplinarias necesarias, las cuales están sujetas al Reglamento Interno de Trabajo de DACTA.

4. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
N/A	N/A	N/A	N/A

5. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
2	20/09/2021	Modificación	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
3	22/02/2023	Actualización	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
3	22/02/2024	Revisión	**Oficial de Seguridad de la Información**	**Comité SIG**	**Gerente General**
Firmas de la versión vigente			 S. Rafaile	 S. Rafaile  A. Morales	 G. Rafaile

Identificación de las modificaciones	
Versión	**Descripción de cambios**
2	Se insertó **3.5 INFORMACIÓN PARA LAS PRUEBAS**
3	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022. Se adicionó el párrafo 3. del capítulo 3.12