Guía - Política seguridad en los procesos de desarrollo y soporte

Contenido

1 Objetivo

Asegurar que la seguridad digital esté diseñada y sea implementada en el ciclo de vida planeación y desarrollo de los sistemas de información del MEN.

2 Alcance

Esta guía política aplica para todos los desarrollos de sistemas de información nuevos y mejoras a los existentes en el MEN.

3 Definiciones

- **Integridad:** Propiedad de la información que consiste en mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Disponibilidad:** Propiedad de la información que consiste en garantizar el acceso y uso de la información y los sistemas de tratamiento de esta a los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** Propiedad de la información que consiste en garantizar que esta sólo es accedida por personas o sistemas autorizados.
- **Criptografía:** Es la ciencia que estudia la transformación de la información mediante algoritmos, protocolos y sistemas con el fin de protegerla y dotar de seguridad a las comunicaciones y a las entidades que se comunican.
- **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Dato:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **MEN:** Ministerio de Educación Nacional
- **OTSI:** Oficina de Tecnología y Sistemas de Información del MEN
- **SGSI:** Sistema de Gestión de Seguridad de la Información del MEN.
- **Seguridad digital:** Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante; incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **Vulnerabilidad:** Es la debilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Incidencia:** Es toda interrupción o reducción de la calidad no planificada del servicio.

4 Directrices

4.1 Seguridad en los procesos de desarrollo y soporte

Objetivo:

Asegurar que la seguridad digital esté diseñada y sea implementada en el ciclo de vida planeación y desarrollo de los sistemas de información del MEN.

4.2 Política de Desarrollo seguro

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	**1 Fase I Planificación - Análisis – Diseño de Sistemas en el MEN** En esta fase se deben considerar los siguientes aspectos: • Definir el alcance • Especificar los atributos de calidad en seguridad que debe cumplir la arquitectura, así como las métricas a utilizar y los rangos de valores aceptables para el MEN. • Especificar la estructura y los requerimientos • Realizar el levantamiento de información • Efectuar el análisis de la información recolectada • Solicitar la Infraestructura que se requiere para los Ambientes de Desarrollo y Prueba.	Oficina de tecnología y sistemas de información Operador TI (Aplicaciones, Fábrica de software, Seguridad)	Manual de Seguridad Digital y Guías de Política. Protocolo de ciclo de vida del software. Documentación de los proyectos de sistemas de información.
	1.1 Requisitos de Seguridad Identificar los objetivos y requisitos de seguridad que se deben contemplar e implementar; estos se determinan de la siguiente forma: 1. Arquitectura de la aplicación. 2. Plataforma donde correrá la aplicación. 3. Tipos de datos que se almacenarán, consultarán o transferirán, es decir se debe definir cuáles son confidenciales y/o públicos de acuerdo con la clasificación de	Oficina de tecnología y sistemas de información Operador TI (Aplicaciones, Fábrica de software, Seguridad)	Documentación de los proyectos de sistemas de información.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	información que tiene el MEN. 4. Tipos de registro que el sistema debe generar, acceso a los recursos, niveles de privilegios, perfiles de usuario. Los tipos de acceso a los datos deben ser estructurados de acuerdo con los perfiles definidos, lectura, escritura, modificación y eliminación. 5. Definir cómo será el modo de autenticación al ingreso al aplicativo, por ejemplo, usuario y contraseñas, tokens, entre otros. 6. En esta etapa es necesario identificar los riesgos del proyecto entre los cuales se deben contemplar, entre otros, los siguientes: • El tiempo designado para el desarrollo no es suficiente, es decir mala planeación en la calendarización. • Reuniones no suficientes y poco productivas. • Inhabilidad o incapacidad durante el desarrollo por parte de un integrante del grupo. • Mala definición de la información confidencial y pública, así como los roles y permisos. • Priorización errónea de las actividades a realizar por cada uno de los integrantes. • Ausencia o demora de respuestas en el trabajo asignado. • Conflictos frecuentes que pueden ser originados por un mal ambiente de trabajo al interior del grupo. • Definición poco clara de los requerimientos. • Documentación de los requerimientos incompleta. • Problemas con alguno de los diseños. • Conflictos con la trazabilidad y/o priorización de los requerimientos • Fallas en la documentación de algún diagrama. • Falta de comunicación con los líderes del proyecto.		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	• Baja disponibilidad por parte de los líderes del proyecto. 7. También se deben definir las acciones correctivas y/o preventivas que se tendrán en el proyecto, tales como: • Establecer tiempos con holgura previendo imprevistos y/o asumir el tiempo adicional requerido y hacer las notificaciones pertinentes. • Establecer compromisos y los temas a tratar antes de las reuniones, enviar previamente la documentación respectiva para que todos tengan conocimiento de lo que se tratará en las reuniones y/o solicitar mediación, de los superiores encargados del proyecto. • Definir responsables que pueden suplir la ausencia de las personas que integran el grupo inicial de definición de requerimientos y/o determinar el tiempo que se prolongaría el proyecto. • Es recomendable que se contemple y adicione en el cronograma de actividades el tiempo correspondiente a la curva de aprendizaje de la persona que se incorpore. Esto es especialmente importante para las actividades que puedan ser desarrolladas directamente por esta persona sin depender del resto del equipo. Para esto, se deben tener en cuenta las habilidades y conocimientos con los que debe contar la persona incorporada. • Las personas intervinientes en el proceso deben tener conocimiento claro de cuál es la información con la cual se trabajará, su disponibilidad y los niveles de importancia para garantizar el cumplimiento de los requisitos de seguridad o, en su defecto, asumir que no se valoraron ni se priorizaron los requerimientos, ni se clasificaron correctamente la información, los roles ni permisos. • Establecer compromisos con los líderes y los usuarios que solicitan el requerimiento, así como definir el proceso para escalar los problemas de incumplimiento de las actividades por parte de los intervinientes del		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	proyecto.		
	1.2 Validar el cumplimiento de los requisitos definidos en la Fase I Planificación - Análisis – Diseño de Sistemas en el MEN. Validar el cumplimiento de los requisitos mediante la aplicación de la Lista chequeo Fase I Planificación - Análisis – Diseño de sistemas seguros en el MEN.	Oficina de tecnología y sistemas de información	Listas de chequeo de verificación de las fases del desarrollo y mantenimiento de software.
	2.1 Requisitos de Seguridad para la Fase II o Contar con ambientes de desarrollo, pruebas y producción y estos deben ser independientes. Estos ambientes deben ser lo más similar posible y con los mismos controles de seguridad, a efectos de prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores en el ambiente de pruebas y producción. o Los desarrolladores deben realizar su trabajo exclusivamente en ambiente de desarrollo, nunca en otros ambientes directamente. o Los nombres de dominio para los ambientes desarrollo, pruebas y producción deben ser diferentes a efectos de evitar confusión durante la ejecución desarrollo, pruebas, y puesta en producción. o Es necesario que se tenga instalado el mismo manejador de base de datos y versión en los ambientes de prueba y producción. Si esto no es posible, usar herramientas automatizadas de propagación de una base de datos a otros. o Incluir réplicas de todos los componentes con los cuales el software tendrá interoperación en producción incluyendo: otras aplicaciones cliente servidor, bases de datos relacionales, componentes middleware, interfaces, demonios (daemons), procesos personalizados, utilidades FTP y otros. **2.1.1 En desarrollo**	Oficina de tecnología y sistemas de información Operador TI (Aplicaciones, Fabrica de software, Seguridad)	Documentación de los proyectos de sistemas de información.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Autentificar adecuadamente: La información confidencial y los sistemas informáticos sólo deben ser accesibles por las personas con los roles y permisos definidos en la fase I. ○ No utilizar campos ocultos para almacenar información sensible, porque esto permitiría que se exponga datos e información del funcionamiento interno de los aplicativos, permitiendo que sean manipulados ○ En caso de que se requiera hacer uso de campos ocultos, debe justificarse por qué es la única alternativa técnica posible, y se debe garantizar que la información almacenada en ellos no sea confidencial o sensible; si esto no es posible, se deben utilizar mecanismos de cifrado con el fin de que se garantice su integridad y confidencialidad. ○ Comprobar las entradas: Es necesario que se verifique y controle los datos que son introducidos en los aplicativos, estos deben estar dentro del rango de valores válidos para el tipo de dato, es decir si son de tipo numérico que lo sean y que no sobrepasen la longitud determinada, sobre todo en los que son tipo cadena. ○ Valores límite de salida: Aquí se debe controlar la salida de los métodos, que el dato resultante de una operación esté dentro de los parámetros definidos antes de asignarlo. ○ Formato de salida: Los formatos de salida no deben ser cambiados por funciones debido a que estos pueden ocasionar errores asociados con el manejo del buffer. ○ Validar los argumentos que se pasan a un componente en otro ámbito de control con el fin de que no se introduzcan argumentos alternativos, utilizando la misma codificación de caracteres, validando los datos resultantes de una combinación de datos de diferentes fuentes, ya que los datos individuales pueden haber pasado la validación, pero violar las restricciones una vez hayan sido combinados ○ Asegurar que los métodos que llevan a cabo controles de seguridad sean declarados como privados o finales, prohibiendo la extensión de los mismos ya que las clases no finales pueden verse comprometidas si una subclase maliciosa reemplaza los métodos y omite las comprobaciones.	Operador TI (Aplicaciones, Fabrica de software, Seguridad)	

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Proteger la información que se muestra sobre los procesos activos ya que muchos sistemas operativos permiten a un usuario observar la información de procesos que pertenecen a otros usuarios. Esta información puede incluir argumentos de línea de comandos o la configuración de la variable de entorno, lo que puede provocar un ataque contra el software por parte de otros usuarios si entre esos datos se incluye información confidencial. ○ Evitar el uso de datos reales de carácter personal en las pruebas anteriores a la implantación o modificación de un sistema, salvo que se garantice el nivel de seguridad correspondiente al tipo de información tratada. ○ Evitar que el usuario tenga acceso a alguna referencia directa a un objeto de la aplicación, como un archivo, directorio, base de datos, o clave, como un parámetro del URL o dentro de un formulario, es decir se debe utilizar mapas de referencias indirectas para referencias objetos del servidor, empleando contraseñas que garanticen que el usuario que intenta acceder al recurso dispone de los permisos suficientes, así como evitar la publicación directa de recursos a través del acceso directo mediante una URL que pueda ser predicha. ○ Evitar generar código a partir de valores ingresados por el usuario. ○ Utilizar Stored Procedures en lugar de sentencias SQL dinámicas. ○ Controlar que los datos de salida sean adecuados, es decir, que cumplan con lo solicitado en los requerimientos, como por ejemplo que el valor obtenido se encuentre dentro de los parámetros definidos. Si esta acción no se tiene en cuenta puede hacer que la funcionalidad desarrollada falle o regrese un resultado que no corresponda, así como permitiendo que el aplicativo no realice las acciones requeridas. **2.1.2 Buenas Prácticas de Desarrollo de Software** ○ Utilizar sistemas de control de versiones y de gestión de configuración		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Emplear nombres descriptivos, en la declaración de variables, es decir, que hagan alusión a su nombre y no a su tipo. ○ Evitar el uso de variables Globales, dado que se puede acceder a estas variables por terceras funciones ya sea por malicia o por infortunio asignando un valor no deseado, este tipo de variables puede ser accedido por muchas funciones durante la ejecución del programa, siendo muy difícil de detectar las fallas que genera. ○ Inicializar siempre las variables. ○ La aplicación deberá generar y almacenar un log de auditoria sobre las tablas y transacciones críticas, que permita consultar como mínimo: ID de usuario, fecha, hora, nombre de la máquina donde ejecutó la aplicación, dirección IP, MAC, tabla modificada, acción ejecutada (creación, modificación, borrado). Si el volumen de datos y la carga transaccional de la aplicación no es muy elevada es aconsejable registrar los valores anteriores y actuales. ○ Los comentarios que contenga el código fuente deben ir enfocados a describir la funcionalidad que se está programando, en los bloques de código extenso es recomendable dividirlos e introducir un comentario al principio con el fin de guiar al desarrollador, sería óptimo que exista una línea blanca de separación, estos comentarios no deben ser excesivos, es decir describiendo lo obvio. ○ Reutilización de Código Fuente: En lo posible se recomienda la reutilización de código fuente cuya calidad haya sido verificada, ya que la no reutilización de código induce a errores cada vez que se desarrolla un nuevo componente de la solución. En caso de requerir funciones de seguridad específicas es recomendable hacer uso de librerías y/o piezas de código ya construidas para tal fin, con el fin de aprovechar la experiencia de los desarrolladores especializados en estas áreas. ○ No excederse con el número de niveles en las instrucciones anidadas. ○ No mezclar datos con código. ○ Evitar usar métodos con muchos parámetros, en caso de que sea necesario es recomendable contemplar la creación de una clase que contenga las propiedades requeridas.		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ No hacer comparaciones explícitas con expresiones booleanas con true o false, es mejor asignar la condición a una variable y utilizar la variable en las comparaciones, nombre las variables de forma afirmativa. ○ Se deben validar todos los parámetros de las interfaces de programación de aplicaciones (API) exportadas, verificando que sean válidos, esto incluye los datos que parecen ser coherentes pero que están más allá del intervalo de valores aceptado, como los tamaños de búfer excesivos. No utilice aserciones para comprobar los parámetros de las API exportadas, porque las aserciones se quitarán en la versión de lanzamiento. ○ Se debe considerar emplear las API criptográficas desarrolladas por firmas reconocidas (IBM, Microsoft, entre otros.) o por la académica, en lugar de escribir a su propio software criptográfico, con ello los desarrolladores podrán concentrarse en la generación de aplicaciones. ○ Cuando una funcionalidad se requiera implementar en diferentes aplicaciones se recomienda crear una función, una rutina, un servicio o un componente que sea reutilizable para cualquier aplicación. ○ Todas las comunicaciones deben ser seguras.		
	2.1.3 En Verificación de Cumplimiento de Especificaciones del Sistema En esta fase se deben contemplar las siguientes recomendaciones: ○ Las pruebas iniciales se deben realizar a partir de los requerimientos y los atributos ded calidad definidos y aprobados. El alcance de estas pruebas es validar que el sistema cumple con los atributos de calidad, el funcionamiento esperado y los requisitos de seguridad de acceso al sistema, a los datos y procesos definidos, así como a los distintos recursos del sistema. ○ Las pruebas funcionales deben ser coherentes con las funcionalidades solicitadas y deben buscar descartar errores que se presenten al utilizar el aplicativo o el módulo desarrollado.	Oficina de tecnología y sistemas de información	Documentación de los proyectos de sistemas de información.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ En caso de que el requerimiento provenga de un mantenimiento es necesario verificar todas las funcionalidades del sistema que se puedan afectar por la integración de la nueva funcionalidad o la solución del problema que dio origen al mantenimiento. ○ También es necesario probar el control de acceso al aplicativo, con el fin de valorar que únicamente accedan los usuarios autorizados y sólo a los módulos definidos de acuerdo con su rol. ○ Las pruebas de seguridad funcional se deben basar en los requerimientos definidos con respecto a: • Autenticación solicitada, complejidad de contraseñas basada en la política definida en este documento y restricciones de acceso según lo diseñado en roles y permisos. • Bloqueo automático de cuentas de acceso. • Funcionalidad de captchas (verificar que el usuario que está accediendo a determinados datos es un humano y no una máquina). • Lo registrado en los logs, así como su almacenamiento. • Los mensajes de error que se deben presentar en las acciones validadas. ○ Al preparar los datos para pruebas, estos preferiblemente no deben ser reales; sin embargo, teniendo en cuenta que para algunas pruebas puede ser una tarea compleja la preparación manual de datos y que puede ser ineficiente debido a la integridad referencial que deben mantener las relaciones de los registros y llegase a ser necesario emplear información real para las pruebas, esta información debe ser anonimizada, con el fin de preservar la confidencialidad de la información empleada. ○ Adicionalmente a los datos de prueba, sean creados o los reales anonimizados, se deben realizar pruebas utilizando variaciones no válidas de éstos en los diferentes módulos de la aplicación en donde se solicite datos, es decir, con diferente signo, tipo, longitud, fuera del rango solicitado, caracteres especiales, valores nulos y/o		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	aleatorios. Esto con el fin de garantizar que la aplicación es robusta y responde apropiadamente a datos inválidos. o Es necesario realizar pruebas de rendimiento de software, estructurando escenarios que sometan la aplicación a su máximo rendimiento y consumo de recursos para verificar que se cumplen con los atributos de calidad apropiados. o Para las pruebas que se realicen a los aplicativos Misionales del MEN, deben ser realizadas por una persona diferente al desarrollador que implementó el requerimiento. o Aunque el proyecto haya tenido que ajustar y actualizar su cronograma por ampliación o reducción de tiempo, nunca se debe recortar el tiempo destinado para las pruebas. Se debe asegurar siempre que el proyecto que se entregue esté libre de errores, y, si se recorta el tiempo en pruebas, pueden presentarse muchos más errores de los habituales. o No se debe publicar ningún aplicativo sin la debida aprobación de acuerdo con los procedimientos establecidos.		
	2.1.4 Validar el cumplimiento de los requisitos definidos en la Fase II Desarrollo – Verificación de Cumplimiento de Especificaciones del Sistema- Verificar Software Seguro- Realizar la publicación del Software en ambiente de preproducción y gestionar aprobación del área funcional. Validar el cumplimiento de los requisitos mediante la aplicación de la Lista chequeo Fase II Desarrollo – Verificación de Cumplimiento de Especificaciones del Sistema- Verificar Software Seguro- Publicar el Software en el ambiente de preproducción y gestionar aprobación del área funcional en el MEN.	Oficina de tecnología y sistemas de información	Listas de chequeo de verificación de las fases del desarrollo y mantenimiento de software.
	3. Fase III - Sensibilizar el uso del sistema de información, Realizar la puesta en producción del Sistema de Información o Mantenimiento de Software, Realizar el mantenimiento de software o atención a incidencias del sistema de información. En esta fase se contemplarán:	Oficina de tecnología y sistemas de información	Documentación de los proyectos de sistemas de información.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Sensibilizar a los usuarios sobre el uso del sistema de información. ○ Poner en producción el Sistema de Información nuevo o actualizado en la operación de mantenimiento. ○ Realizar el mantenimiento de software o dar atención a incidencias del sistema de información.		
	3.1 Requisitos de Seguridad para la fase III Contemplar los siguientes aspectos al realizar la sensibilización o transferencia de conocimiento en la puesta en producción: ○ Las políticas de seguridad de la información. ○ La importancia del buen uso del aplicativo. ○ La confidencialidad que maneja el aplicativo ○ Las restricciones, roles y perfiles, manejos de usuarios y contraseñas con los que va a contar el aplicativo. ○ Los aplicativos Misionales del MEN publicados en el ambiente de producción deben incluir los mecanismos de seguridad en tres grupos: • Prevención: Evitando desviaciones respecto a la política de seguridad del Ministerio de Educación Nacional. • Detección: Mostrando las desviaciones, violaciones o intentos de violación, si se producen, de la seguridad del sistema donde se encuentran ubicados los aplicativos Misionales del Ministerio de Educación Nacional. • Recuperación: Los cuales deben ser aplicados cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. ○ Contemplar los lineamientos de seguridad planteados en el presente documento en todos los mantenimientos o incidencias que se presenten, así como en su	Oficina de tecnología y sistemas de información	Documentación de los proyectos de sistemas de información.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	implementación la confidencialidad, integridad y disponibilidad que afecten o modifiquen estos requerimientos.		
	3.2 Validar el cumplimiento de los requisitos definidos en la Fase III Sensibilizar el uso del sistema de información, Realizar la puesta en producción del Sistema de Información o Mantenimiento de Software, Analizar el mantenimiento de software o atención a incidencias del sistema de información. Efectuar la validación del cumplimiento de los requisitos mediante la aplicación de la Lista chequeo Fase III Sensibilizar el uso del sistema de información, Realizar la puesta en producción del Sistema de Información o Mantenimiento de Software, Analizar el mantenimiento de software o atención a incidencias del sistema de información en el MEN.	Oficina de tecnología y sistemas de información	Listas de chequeo de verificación de las fases del desarrollo y mantenimiento de software.

4.3 Procedimientos de control de cambios en sistemas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES

Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Documentar y hacer cumplir los procedimientos formales de control de cambios que se tienen definidos en el MEN, para asegurar la integridad del sistema, las aplicaciones y los productos, desde las primeras etapas de diseño a través de todos los esfuerzos de mantenimiento posteriores. Este proceso debe incluir: ✓ Una valoración de riesgos de seguridad digital. ✓ Análisis de los impactos de los cambios y la especificación de los controles de seguridad. ✓ El uso de un sistema de gestión de versiones, que permita recuperar versiones especificas cuando se requiera.	Oficina de tecnología y sistemas de información	Comités CAB y ECAB
	Propender por el cumplimiento del Procedimiento de gestión de cambios ST-PR-12 y el Instructivo Lineamientos Gestión de cambios ST-IN-03 definidos en el MEN para asegurar la integridad del sistema, las aplicaciones y los productos, desde las primeras etapas de diseño a través de todos los esfuerzos de mantenimiento posteriores.		Procedimiento de Gestión de Cambios ST-PR-12 Instructivo Lineamientos Gestión de cambios ST-IN-03
	Exigir que en los nuevos sistemas y cambios importantes a los sistemas existentes se ejecute un proceso formal de documentación, especificación, pruebas, control de calidad y gestión de la implementación.		

4.4 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES

Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del MEN, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad del MEN	Garantizar que cuando se cambian las plataformas de operación (sistemas operativos, bases de datos, plataformas de middleware y aplicaciones), se revisan las aplicaciones críticas del negocio, y se prueban para asegurar que no haya impacto adverso en las operaciones o seguridad del MEN. Esto debe comprender: ○ Revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones. ○ Garantizar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación. ○ Garantizar que se hacen cambios apropiados en los planes de continuidad del negocio. ○ Garantizar que los cambios realizados en sistemas de información se revisan escaneando vulnerabilidades y mitigándolas.	Oficina de tecnología y sistemas de información Operador de servicios TI (Aplicaciones, Infraestructura, Seguridad)	Procedimiento de Gestión de Cambios ST-PR-12 Instructivo Lineamientos Gestión de cambios ST-IN-03 ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas.

4.5 Restricciones en los cambios a los paquetes de software

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los	Controlar las modificaciones al software del MEN, las cuales se deben limitar a los cambios necesarios. En donde un software necesite modificaciones, se deben considerar los siguientes puntos: ○ Se debe contar con sistema de gestión de versiones que permita recuperar versiones previas en caso de ser necesario.	Oficina de tecnología y sistemas de información	Procedimiento de Gestión de Cambios ST-PR-12 Instructivo Lineamientos Gestión de cambios ST-IN-03

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ El riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos; ○ Tener el consentimiento del proveedor (vendedor). ○ Obtener del proveedor (vendedor) los cambios requeridos, a medida que se actualiza el programa estándar; ○ El impacto, si el MEN llega a ser responsable del mantenimiento futuro del software como resultado de los cambios; ○ La compatibilidad con otro software en uso en el MEN.		
	Implementar un plan de gestión de actualizaciones de software para asegurar que se instalen las actualizaciones de aplicaciones y de parches aprobados más recientes para todo el software autorizado.		Plan de actualizaciones Contrato con el operador de TI.
	Exigir que todos los cambios se prueben y documenten completamente, de manera que se puedan aplicar nuevamente, si es necesario, a futuras actualizaciones de software.		Procedimiento de Gestión de Cambios ST-PR-12 Instructivo Lineamientos Gestión de cambios ST-IN-03
	Requerir en todos los cambios el escaneo de vulnerabilidad y el plan para la mitigación de estas.		Procedimiento de Gestión de Cambios ST-PR-12 Instructivo Lineamientos Gestión de cambios ST-IN-03 Escaneo de vulnerabilidades y plan de mitigación.

4.6 Principios de construcción de los sistemas seguros

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Establecer, documentar y aplicar lineamientos de construcción de sistemas de información seguros, basados en principios de desarrollo seguro en el MEN. Tener en cuenta los siguientes principios de construcción de sistemas de información seguros: ○ Partir siempre de un modelo de permisos mínimos, es mejor ir escalando privilegios por demanda de acuerdo con los perfiles establecidos en las etapas de diseño. ○ Todos los accesos que se hagan a los sistemas deben ser validados. ○ Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido. Si se utiliza un lenguaje compilado, se debe garantizar que la compilación se realiza utilizando las mejores optimizaciones disponibles y que no se incluya información para depuración. ○ Deben incluir pruebas de cubrimiento del código para garantizar que todo el código es probado. ○ La seguridad se debe incluir en el diseño de todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad digital, con la necesidad de accesibilidad.	Oficina de tecnología y sistemas de información Operador de servicios TI (Aplicaciones, Infraestructura, Seguridad)	Manual de Seguridad Digital - Guías de Política

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Nunca confiar en los datos que ingresan a la aplicación, todo dato debe ser verificado para garantizar que lo que está ingresando a los sistemas es lo esperado y además evitar ataques por inyección de código. ○ Cualquier funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo con los requerimientos de diseño. De esta forma se evita tener porciones de código que resultan siendo innecesarias. ○ Cualquier cambio que se haga debe quedar documentado, esto facilitará modificaciones futuras. ○ Como parte de las actividades del ciclo de vida del desarrollo SDL se deben tomar como referencias prácticas reconocidas de desarrollo seguro, por ejemplo: Microsoft SDL, OWASP, SANS CWE Top 25, CERT Secure Coding, entre otras. El desarrollo de software debe estar alineado con los requerimientos de seguridad establecidos contractualmente, por normativas o regulaciones aplicables al MEN. ○ Para intercambiar información sensible, se deben utilizar protocolos seguros para cifrar las comunicaciones. En el caso de almacenamiento la información confidencial debería estar cifrada utilizando algoritmos fuertes y claves robustas. ○ Los principios y los procedimientos de construcción establecidos se deben revisar con regularidad para asegurar que están contribuyendo efectivamente a mejorar los estándares de seguridad dentro del proceso de construcción de software en el MEN. ○ Haber pasado por un proceso completo de pruebas (técnicas, funcionales, seguridad, etc.) y certificación los sistemas de información del MEN, antes de ser liberados a producción en un ambiente dedicado para tal fin.		

4.7 Ambiente de desarrollo seguro

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Exigir a los proveedores en los desarrollos de software para el MEN, que deben contar con ambientes independientes tales como: pruebas, certificación y producción, estos deben contemplar controles físicos y de acceso lógico para asegurar la separación de estos. (Aplica para sistemas de informacion nuevos o existentes) Los controles que se deben tener en cuenta: ○ Los datos almacenados en el ambiente de producción no deben ser utilizados para las actividades de certificación o pruebas. ○ Los datos utilizados en los ambientes de desarrollo, pruebas, certificación no deben ser los utilizados en el ambiente de producción. ○ Habilitar solo los módulos, servicios, protocolos y aplicaciones que sean necesarias para el buen funcionamiento del sistema de información. Aquellos que no se utilicen deberán ser deshabilitados. El desarrollador es responsable de documentar cuáles son estrictamente necesarios para el correcto funcionamiento del aplicativo. ○ Verificar que los aplicativos cuenten con las últimas versiones estables, tanto a nivel de software como de sistema operativo, parches de seguridad, servidor de aplicaciones, base de datos, máquina virtual de java, etc., antes del despliegue. ○ Verificar que no se pueda listar los directorios de la aplicación. ○ Verificar que en el servidor no se encuentren instalados módulos, extensiones, programas por defecto y que no serán usados por la aplicación. ○ Controlar para que los usuarios no tengan acceso a aquellos archivos de configuración o a directorios sensibles que no puedan ser eliminados. Solo usuarios con privilegios o autorizados deberán tener acceso.	Oficina de tecnología y sistemas de información	Contratos con los proveedores de desarrollo de software Informe de ejecución de los contratos con los proveedores de desarrollo de software

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Controlar para que todos los usuarios de la aplicación y el software que se ejecuten en el servidor (base de datos, sftp, apache, iis, jboss, tomcat, etc.) tengan los mínimos privilegios sobre el sistema. ○ Garantizar que no se permita la transferencia de archivos con configuraciones del sistema a los usuarios. ○ Controlar si la aplicación requiere que el usuario adjunte archivos, verificar que solo este permitido el envío de documentos con extensiones específicas, por ejemplo: doc, docx, pdf. No permitir que el usuario adjunte archivos con extensiones asp, txt, php, jsp, exe, etc. ○ Validar los archivos enviados al servidor por el usuario en la estructura de su cabecera, ya que la extensión puede ser falsificada por este. ○ Controlar para que los archivos que son enviados por el usuario no sean almacenados en el mismo entorno de trabajo de la aplicación, se recomienda guardarlos en un dispositivo aislado. ○ Controlar y de ser posible solo permitir el cargue de archivos .pdf a los sistemas de información y, en la medida de lo posible, no deben incluir scripts. ○ Controlar para que los archivos transferidos al servidor por el usuario no se almacenen con permisos de ejecución, sólo de lectura. ○ No utilizar rutas especificas en los parámetros o variables, se recomienda, utilizar índices que internamente se asocien a directorios o rutas predefinidas. ○ utilizar protocolos seguros, tales como SSH, SFTP, FTPS, VPN SSL, IP SEC, etc. Para la comunicación y transferencia de archivos. ○ Todos los sistemas que implementen Web Services dentro de su funcionamiento, deben contar con mecanismos de seguridad adecuados. Se deben tener en cuenta los siguientes aspectos, sin limitarse a: ○ Configurar solo métodos HTTP seguros, tales como POST. No permitir el uso de los métodos DELETE, PUT, GET, y TRACE. ○ Implementación de soporte HTTPS para mensajes tipo SOAP.		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	▪ Cifrado y firma de contenido XML. ▪ Implementación de especificaciones de seguridad como: WS-Security, WSTrust, WS-Signature, XML Encryption, SAML, ebXML, WS-policy. ▪ Validación de entradas. ▪ Validación de XML según el esquema definido. ▪ Generación de logs de las transacciones de los Web Services. o Modificar las cabeceras HTTP para que no muestre información sobre las versiones y las aplicaciones que se encuentran en el servidor. Por ejemplo: modificar la cabecera “Server”.		

4.8 Desarrollo contratado externamente

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados	Supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente por el MEN.	Oficina de tecnología y sistemas de información	Informe de supervisión a los contratos con los proveedores de desarrollo de software
	Verificar y hacer cumplir por parte del tercero los siguientes puntos en toda la cadena de suministro del MEN: o Los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.		Informe de supervisión a los contratos con los proveedores de desarrollo de software

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas. ○ El suministro del modelo de amenaza aprobado al desarrollador externo. ○ Las pruebas de aceptación para determinar la calidad y exactitud de los entregables. ○ La entrega de evidencias de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad. ○ La entrega de evidencias de que se han hecho pruebas suficientes para garantizar que el sistema está protegido contra contenido malicioso intencional y no intencional en el momento de la entrega. ○ La entrega de evidencias de que se han hecho pruebas suficientes para garantizar que el sistema está protegido contra la presencia de vulnerabilidades conocidas. ○ Derecho contractual con relación a procesos y controles de desarrollo de auditorías. ○ Documentación eficaz del ambiente de construcción usado para crear los entregables. ○ Aceptar las políticas y procedimientos que se encuentran dentro de este documento. ○ Cumplir con el procedimiento del protocolo de paso a producción.		
	Realizar para todos los sistemas desarrollados, un proceso de verificación de código antes de su salida a producción, incluyendo aquellas librerías de terceros que son incluidas en el desarrollo (DLL).		ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Establecer programas de prueba para aceptación y criterios de aceptación relacionados para los sistemas de información nuevos, actualizaciones y nuevas versiones.		Programas de prueba.

4.9 Pruebas de seguridad de sistemas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Se deben tener en cuenta las siguientes consideraciones al realizar pruebas de seguridad: ○ Las revisiones de código pueden ser realizadas por terceros contratados para tal efecto, o por personal interno capacitado para hacerlo con el fin de asegurar la idoneidad de quien realiza dicha actividad. ○ Puede realizarse a través de herramientas automáticas o mediante técnicas manuales. ○ Los cambios en el código fuente deben ser revisados por personas diferentes al autor de este, con conocimiento en técnicas de verificación de código y desarrollo seguro. ○ Las revisiones de código deben estar orientadas a verificar que la codificación cumpla con todos los requerimientos expuestos en la presente política. ○ Las observaciones generadas en la revisión deben ser atendidos antes de la puesta en producción del sistema. ○ Los procesos de revisión deben alinearse a los requerimientos de normativas y regulaciones aplicables al MEN. ○ Una evaluación del riesgo de vulnerabilidades en el código debe realizarse y valorarse con los interesados en el software creado.	Oficina de tecnología y sistemas de información	ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas. Pruebas de Seguridad Pruebas de Stres

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Verificar que los aplicativos cuenten con las últimas versiones estables, tanto a nivel de software como de sistema operativo, parches de seguridad, servidor de aplicaciones, base de datos, máquina virtual de java, etc., antes del despliegue.		ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas.
	Realizar por lo menos una revisión del código antes de liberarlo en producción, y poder llevar a cabo las actividades de remediación y seguimiento a estas vulnerabilidades antes que salga a producción. En este proceso se deben tener en cuenta las vulnerabilidades más importantes en la industria (OWASP Top 10, CWE Top 25, etc.).		ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas.

4.10 Pruebas de aceptación de sistemas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para	Establecer programas de prueba para aceptación, escaneo de vulnerabilidades y criterios de aceptación relacionados para los sistemas de información nuevos, actualizaciones y nuevas versiones. Definir y ejecutar las pruebas de aceptación de software a partir de los siguientes elementos: • Requerimientos del usuario. • Requerimientos de sistema. • Casos de uso. • Procesos de negocio.	Oficina de tecnología y sistemas de información	ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas. Pruebas de Seguridad Pruebas de Stres

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	• Atributos de calidad. • Reportes de análisis de riesgo. • Requisitos de seguridad de la información.		
	Incluir en las pruebas de requisitos de seguridad de la información los siguientes puntos: • Llevarse a cabo sobre componentes y sistemas integrados. • Hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y verificar que se han corregido los defectos relacionados con la seguridad. • Realizar una prueba de intrusión, en ambiente productivo definitivo, pero con acceso controlado con el fin de conocer y evaluar las condiciones de seguridad que rodean el ambiente final con el fin de hacer ajustes finales, el responsable de esta revisión debe ser una persona diferente al desarrollador (Por ejemplo: revisión por pares). • Realizar pruebas de Ethical Hacking antes de salir a producción. Al identificar una vulnerabilidad técnica en el proceso de desarrollo de un sistema, se debe identificar el riesgo asociado y el plan de acción para remediarla.		ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas. Pruebas de Seguridad Pruebas de Stres Planes de Pentest

4.10.1 Gestión de vulnerabilidades

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Para los sistemas de información nuevos, actualizacione	Realizar por lo menos una revisión del código antes de liberarlo en producción, o para cambios entre ambientes para así poder llevar a cabo las actividades de remediación y seguimiento a estas vulnerabilidades antes que salga a producción. En este proceso se deben tener en cuenta las vulnerabilidades más importantes en la industria (OWASP Top 10, CWE Top 25, etc.).	Oficina de tecnología y sistemas de información	ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
		Operador TIC Seguridad y aplicaciones	Soluciones Tecnológicas. Escaneo de vulnerabilidades y gestión de la remediación
	Realizar una prueba de intrusión, antes de realizar la puesta en producción o puesta a disposición de usuario final de un sistema aplicación, en ambiente productivo definitivo, pero con acceso controlado con el fin de conocer y evaluar las condiciones de seguridad que rodean el ambiente final con el fin de hacer ajustes finales. El responsable de esta revisión debe ser una persona diferente al desarrollador (Por ejemplo: revisión por pares).		Planes de Pentest

4.11 Protección de datos de prueba

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar la protección de los datos para la prueba	Seleccionar, proteger y controlar cuidadosamente los datos de prueba que se utilicen para los desarrollos de sistemas de información en el MEN.	Oficina de tecnología y sistemas de información Operador TIC Seguridad y aplicaciones	Gestión de solicitudes de datos para pruebas.
	Autorizar específicamente cada copia información operacional a un ambiente de pruebas.		
	Registrar las acciones para realizar el copiado y uso de la información operacional a través de log para suministrar un rastro de auditoría.		
	Evitar el uso de datos operacionales que contengan información de datos personales o cualquier otra información confidencial para propósitos de prueba. Si esta información de datos personales u otra información confidencial se usa para		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	propósitos de las pruebas, todos los detalles y contenido sensibles se deben proteger eliminándolos o modificándolos.		
	Aplicar los procedimientos de control de acceso, que se aplican a los sistemas de información operacionales, también a los sistemas de información de pruebas.		Logs de los sistemas de información – ambientes de pruebas.
	La información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.		Logs de los sistemas de información – ambientes de pruebas.

5. Información de contacto

Cualquier inquietud relacionada con la Guía - Política seguridad en los procesos de desarrollo y soporte, favor remitirla al correo seguridaddigital@mineducacion.edu.co.

6. Revisión de la guía

Esta guía debe ser revisada por la OTSI como mínimo una vez al año.

7. Referentes

7.1 Referentes Normativos

- Dominio A.14 Adquisición, desarrollo y mantenimiento de sistemas
- Objetivo de control A.14.2 Seguridad en los procesos de desarrollo y soporte

7.1.1 Referentes de política nacional

Manual de seguridad y privacidad de la información – Min TIC - Estrategia de Gobierno Digital. Numeral 8.2 Fase de planificación - Políticas de Seguridad y Privacidad de la Información -

7.1.2 Referentes de políticas del MEN

- Manual del Sistema Integrado de Gestión – MEN. Sistema de Gestión de Seguridad de la Información

Control de Cambios		
Versión	**Fecha de vigencia**	**Naturaleza del cambio**
01	A partir de su publicación en el SIG	Se unificó el manual de seguridad informática y el manual de políticas de seguridad de la información y se creó una guía por cada política para especificar las directrices, responsables y soportes.

Registro de aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Luis Carlos Serrano Pinzón	**Nombre**	Lina Mercedes Durán Martínez	**Nombre**	Roger Quirama Garcia
Cargo	Contratista de la Oficina de Tecnología y Sistemas de Información	**Cargo**	Profesional Especializado - Subdirección de Desarrollo Organizacional.	**Cargo**	Jefe de la Oficina de Tecnología y Sistemas de Información