

 ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL <small>Instituto Distrital para la Protección de la Niñez y la Juventud</small>	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACION	CÓDIGO	E-GTIC-PR-010
		VERSIÓN	01
	SEPARACION DE AMBIENTES	PÁGINA	1 de 4
		VIGENTE DESDE	27/12/2024

1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO	
OBJETIVO	Garantizar la seguridad, control y segregación adecuada de los entornos de desarrollo, pruebas y producción dentro del ciclo de vida del desarrollo de software y la gestión de infraestructura tecnológica en IDIPRON. Este procedimiento busca prevenir riesgos de interferencias no deseadas, proteger datos sensibles y garantizar que los cambios en un entorno no afecten a otros, cumpliendo con normativas de seguridad informática
ALCANCE	Este procedimiento aplica a todos los equipos técnicos y administrativos involucrados en el desarrollo, pruebas, implementación y mantenimiento de aplicaciones y sistemas tecnológicos de IDIPRON. Abarca la gestión de los ambientes de desarrollo, pruebas y producción, incluyendo controles de acceso, manejo de datos y monitoreo de actividades...

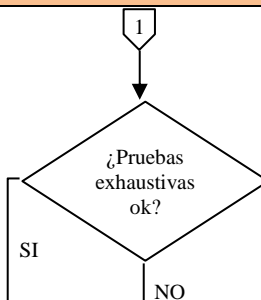
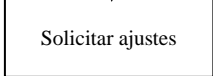
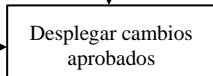
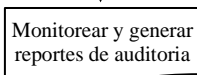
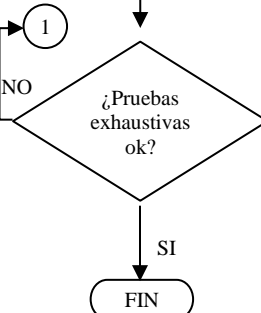
2. GLOSARIO	
Término	Definición
Ambiente de Desarrollo	Entorno tecnológico configurado para el desarrollo de software, donde se crean y prueban nuevas funcionalidades. Debe estar configurado con permisos adecuados y usando datos anonimizados para evitar comprometer información sensible.
Ambiente de Producción	Entorno final en el que se ejecutan los sistemas o aplicaciones para el uso real de los usuarios. Este debe contar con las medidas de seguridad más estrictas, monitoreo
Ambiente de Pruebas	Entorno replicado del ambiente de producción utilizado para realizar pruebas de cambios o nuevas funcionalidades antes de su implementación. Debe estar libre de datos sensibles y ser validado para asegurar su consistencia.
Auditorías Automáticas	Proceso de revisión automatizado que monitorea y registra actividades realizadas en los ambientes, con el fin de detectar y reportar incidentes de seguridad o accesos no autorizados.
Bitácora	Registro continuo y detallado de todas las actividades relevantes que se realizan en los diferentes ambientes, incluyendo configuraciones, cambios y medidas de seguridad. Es utilizado como referencia y control de las acciones ejecutadas.
Control de Accesos Diferenciados	Sistema que asegura que los usuarios solo tengan acceso a los ambientes y funciones que les corresponden según su rol (desarrollo, pruebas, control, administración), limitando los accesos no autorizados.
Despliegue de Cambios	Proceso de implementar los cambios aprobados en el ambiente de producción, realizado en horarios programados para minimizar el impacto en los servicios.
Incidencia	Evento inesperado o error que afecta el funcionamiento de los sistemas o ambientes, que debe ser documentado y corregido para evitar recurrencias.
Informe de Accesos	Documento donde se registra el control de accesos y permisos en los diferentes ambientes, asegurando que solo el personal autorizado tenga acceso y que los permisos estén actualizados.
Informe de Auditoría	Reporte generado periódicamente para auditar las actividades realizadas en los ambientes, detectando y reportando incidentes de seguridad y accesos no autorizados.
Informe de Pruebas Iniciales	Documento que valida la consistencia y adecuación del ambiente de pruebas antes de su implementación definitiva, garantizando que no contiene datos sensibles y replica el ambiente de producción en la medida de lo posible
Informe Técnico	Documento en el que se registra la configuración de los ambientes, pruebas realizadas, cambios implementados y medidas de seguridad adoptadas, asegurando que se cumplen con las condiciones establecidas.
Medidas Correctivas	Acciones tomadas para corregir una incidencia o error detectado, asegurando que no vuelva a ocurrir en el futuro. Estas medidas son aprobadas por el responsable de seguridad y TI antes de ser implementadas.
Monitoreo Continuo	Supervisión constante de todos los ambientes (desarrollo, pruebas y producción) para detectar posibles incidentes de seguridad, errores o problemas en el funcionamiento del sistema.
Permisos de Acceso	Derechos o privilegios asignados a los usuarios para acceder o modificar recursos en los ambientes de desarrollo, pruebas y producción, de acuerdo con su rol o función dentro del proceso
Pruebas de QA (Quality Assurance)	Actividad realizada por el equipo de calidad para asegurar que el software o los cambios sean estables, seguros y funcionen correctamente antes de ser implementados en producción.
Registro de Cambios	Documento que detalla cada uno de los cambios realizados en el ambiente de producción, incluyendo las aprobaciones previas, las incidencias detectadas durante el proceso y el impacto de los cambios implementados.
Validación de Cambios	Proceso mediante el cual se verifican los cambios en el ambiente de pruebas para garantizar que no afecten la estabilidad, seguridad o funcionalidad del sistema antes de su implementación en producción.

	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACION	CÓDIGO	E-GTIC-PR-010
		VERSIÓN	01
	SEPARACION DE AMBIENTES	PÁGINA	2 de 4
		VIGENTE DESDE	27/12/2024

3. CONDICIONES GENERALES	
No.	Descripción
1	Configuración inicial de los ambientes: el/la responsable de la infraestructura tecnológica del IDIPRON debe crear el ambiente de desarrollo asegurándose de que esté configurado con permisos adecuados y utilizando datos anonimizados para evitar comprometer información sensible. Una vez configurado, se valida que el ambiente cumpla con las condiciones técnicas establecidas. Este paso se registra en un informe técnico que debe reposar en el formato BITÁCORA DE REGISTRO DE CAMBIOS E INCIDENCIAS -Cod XXX-XXX-FT
2	Establecimiento del ambiente de pruebas: El/la responsable de la infraestructura configura el ambiente de pruebas replicando, en la medida de lo posible, las condiciones del ambiente de producción. Es fundamental que este ambiente no contenga datos sensibles reales, por lo que deben emplearse datos anonimizados o generados específicamente para las pruebas. Se realiza una validación de consistencia entre los ambientes y se documenta en un informe de pruebas iniciales.
3	Implementación del ambiente de producción: El/la responsable de la infraestructura debe configurar el ambiente de producción con las medidas de seguridad más estrictas, asegurando el monitoreo constante y activando auditorías automáticas el ambiente debe estar protegido contra accesos no autorizados y errores potenciales.
4	Control de accesos diferenciados: sólo se darán permisos a los ambientes según los roles que desempeñen los participantes en cada proceso (desarrollo, control, pruebas, administración), restringiendo permisos de desarrollo y pruebas en el ambiente de producción. Este control se valida mediante revisiones periódicas de permisos, asegurando que sólo el personal autorizado tenga acceso a cada entorno. Los ajustes realizados se documentan en un informe de accesos actualizado. Y deben reposar en la BITÁCORA DE REGISTRO DE CAMBIOS E INCIDENCIAS
5	Validación de cambios en el ambiente de pruebas: Antes de implementar cualquier cambio en el ambiente de producción, el Equipo de QA debe realizar pruebas exhaustivas en el ambiente de pruebas, verificando la estabilidad, seguridad y funcionalidad del cambio. Los resultados de estas pruebas se consolidan en un acta que debe ser revisada y aprobada por los/las responsables técnicos y de seguridad.
6	Despliegue de cambios en producción: Una vez aprobados los cambios, el/la Administrador de TI procede a desplegarlos en el ambiente de producción. Este despliegue debe realizarse en horarios programados para minimizar interrupciones en los servicios. Se documenta el proceso en un registro de cambios, el cual incluye las aprobaciones previas y cualquier incidencia registrada durante la implementación
7	Monitoreo continuo y auditorías: se debe monitorear constantemente los tres ambientes, con especial énfasis en el ambiente de producción. Este monitoreo incluye la generación de reportes de auditoría que detallan actividades realizadas y detectan posibles incidentes de seguridad. Los reportes deben ser revisados periódicamente por el/la encargado(a) de Seguridad, quien puede recomendar ajustes adicionales.
8	Gestión de incidencias y medidas correctivas: Ante cualquier incidencia o anomalía detectada en los ambientes, el Administrador de TI debe documentarla en un informe detallado, especificando las medidas correctivas implementadas. Estas acciones se revisan y aprueban conjuntamente con el/la Líder de Seguridad para asegurar que no se repitan en el futuro.

4. DESARROLLO DEL PROCEDIMIENTO						
No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
1		Crear el ambiente de desarrollo asegurándose de que esté configurado con permisos adecuados y utilizando datos anonimizados.	Responsable de Infraestructura		Informe técnico registrado en bitácora	Prom: 2 días
2		Configurar el ambiente de pruebas replicando las condiciones del ambiente de producción, sin usar datos sensibles reales.	Responsable de Infraestructura		Informe de pruebas inicial	Prom: 3 días
3		Configurar el ambiente de producción con medidas de seguridad estrictas, monitoreo constante y auditorías automáticas.	Responsable de Infraestructura		Informe técnico y de seguridad	Prom: 4 días
4		Revisar los permisos de acceso según los roles de los participantes (desarrollo, control, pruebas, administración).	Responsable de Infraestructura		Informe de accesos actualizado en bitácora	Prom: cada 2 semanas

	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACION	CÓDIGO	E-GTIC-PR-010
		VERSIÓN	01
	SEPARACION DE AMBIENTES	PÁGINA	3 de 4
		VIGENTE DESDE	27/12/2024

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
5		Realizar pruebas exhaustivas en el ambiente de pruebas antes de implementar cualquier cambio en el de producción. Si pruebas satisfactorias se solicita despliegue a producción Si no se solicita ajustes correspondientes	Equipo de QA	X	Acta de validación de pruebas	Prom: 1 día por cambio
6		Reportar los errores detectados	Equipo de QA		Reporte de errores	Prom: 1 día por ciclo de pruebas
7		Desplegar los cambios aprobados en el ambiente de producción en horarios programados.	Administrador de TI		Registro de cambios y incidencias	Prom: 1 día por cambio
8		Monitorear continuamente los tres ambientes y generar reportes de auditoría.	Encargado de Seguridad		Reporte de auditoría de monitoreo	Prom: Diario
9		Se realizan pruebas validación ambiente producción Si se presentan incidencias se documentan así como las medidas correctivas implementadas, asegurando que no se repitan.	Administrador de TI y Líder de Seguridad	X	Informe detallado de incidencias y medidas	Prom: Según incidente

5. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se crea el PROCEDIMIENTO SEPARACION DE AMBIENTES el cual garantiza la seguridad, control y segregación adecuada de los entornos de desarrollo, pruebas y producción dentro del ciclo de vida correspondiente al desarrollo de software y la gestión de infraestructura tecnológica necesarias en el Instituto Distrital Para la Protección de la Niñez y la Juventud IDIPRON/Oficina de TICS, según lo establecido en el decreto 612 de 2018 y en el Decreto 500 de 2020 Por medio del cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.	27/12/2024	YEIMMY ROCIO CARDENAS CRUZ TECNICO OPERATIVO CÓDIGO 314 GRADO 03 WILSON ANDRES RAMIREZ URBINA PROFESIONAL OFICINA DE TIC

	GESTION TECNOLOGIAS DE LA INFORMACION Y COMUNICACION	CÓDIGO	E-GTIC-PR-010
		VERSIÓN	01
	SEPARACION DE AMBIENTES	PÁGINA	4 de 4
		VIGENTE DESDE	27/12/2024

6. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	SANDRA PATRICIA GUERRERO RAMIREZ	ING. GOBIERNO DIGITAL OFICINA DE TIC	27/12/2024
APROBACIÓN LÍDER DE PROCESO	LUIS CARLOS OCAMPO RAMOS	JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIÓN	27/12/2024