



Instituto Nacional de Bosques
Más bosques. Más vida



**INSTITUTO NACIONAL DE BOSQUES -INAB-
GUATEMALA, 27 DE DICIEMBRE DE 2023
RESOLUCIÓN DE GERENCIA NO. 194-2023**

**APROBACIÓN DEL PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL
INSTITUTO NACIONAL DE BOSQUES -INAB-**

La Gerencia del Instituto Nacional de Bosques -INAB-

CONSIDERANDO

Que el Instituto Nacional de Bosques es una entidad estatal, autónoma, descentralizada, con personalidad jurídica, patrimonio propio e independencia administrativa; es el órgano de dirección y autoridad competente del sector público agrícola en materia forestal.

CONSIDERANDO

Que la Ley Forestal, en el Artículo 16 regula las atribuciones del Gerente, que Consisten en: dirigir, ejecutar y ordenar todas las actividades técnicas y administrativas del INAB; con base en las políticas, lineamientos y mandatos establecidos por la Junta Directiva, siendo responsable ante ésta por el correcto y eficaz funcionamiento del Instituto.

CONSIDERANDO

Que es necesario disponer de instrumentos técnicos actualizados que permitan optimizar las actividades y procedimientos institucionales, en función de incrementar la eficiencia y productividad del desempeño de los objetivos y atribuciones del Instituto Nacional de Bosques.

POR TANTO

Esta Gerencia, con base en lo considerado y con fundamento en lo preceptuado en los Artículos: 5, 6 y 16 del Decreto 101-96 del Congreso de la República de Guatemala, Ley Forestal; Artículos 1, 3, 4, y 5 del Reglamento Orgánico Interno del Instituto Nacional de Bosques Acta número JD.48.2022, Resolución JD.02.48.2022.

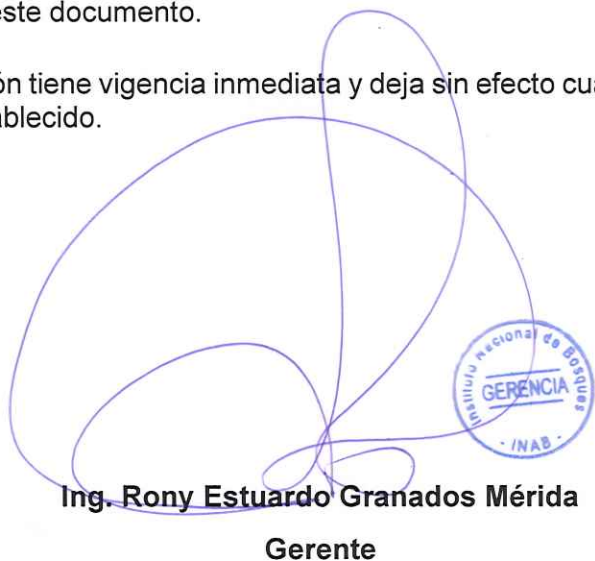
RESUELVE:

- I. Aprobar el Plan de Continuidad de Tecnologías de la Información del Instituto Nacional de Bosques, versión 1, que describe los planes de respuesta para el cumplimiento de la Política de Continuidad de Tecnologías de la información.





- II. El Departamento de Gestión de la Calidad, de la Dirección de Planificación, Evaluación y Seguimiento Institucional, archivará y custodiará en formato físico y digital el original el Plan de Continuidad de Tecnologías de la Información del Instituto Nacional de Bosques, versión 1, debidamente aprobada por el Gerente del INAB.
- III. Se ordena al Jefe (a) de la Unidad de Tecnologías de la Información y Comunicación, realizar la socialización del Plan de Continuidad de Tecnologías de la Información del Instituto Nacional de Bosques, al personal de la Institución.
- IV. Todo funcionario y empleado de la Institución es responsables de la aplicación del Plan de Continuidad de Tecnologías de la Información, con el fin de prevenir, identificar y eliminar los riesgos de interrupción, así como asegurar las condiciones para la recuperación de las operaciones más críticas de la institución en caso de que ocurran, a través de acciones definidas dentro de este documento.
- V. La presente resolución tiene vigencia inmediata y deja sin efecto cualquier otro documento que contrarié lo aquí establecido.
- VI. Notifíquese.

A large, stylized handwritten signature in blue ink. To the right of the signature is a circular official stamp of the INAB Gerencia. Below the signature, the name 'Ing. Rony Estuardo Granados Mérida' and the title 'Gerente' are printed.

Ing. Rony Estuardo Granados Mérida
Gerente



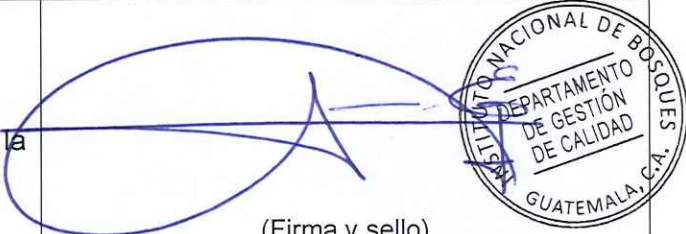


PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE BOSQUES

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Versión: 1
Número de páginas: 13

Elaboró	Aprobó
Jefe (a) de Unidad de Tecnologías de la Información y Comunicación	Gerente
 (Firma y sello)	 (Firma y sello)

Orientación y acompañamiento: Departamento de Gestión de la Calidad	 (Firma y sello)
--	---



Instituto Nacional de Bosques
más bosques, más vida

PRESENTACIÓN

El Instituto Nacional de Bosques -INAB- fue creado mediante el Decreto del Congreso de la República de Guatemala Número 101-96 Ley Forestal, en el año 1996, como el órgano de dirección y autoridad competente del sector público agrícola en materia forestal, teniendo como marco de acción institucional, la administración de los bosques del país fuera de áreas protegidas.

VISIÓN

El Instituto Nacional de Bosques es una institución líder y modelo en la gestión de la política forestal nacional, reconocida nacional e internacionalmente por su contribución al desarrollo sostenible del sector forestal en Guatemala, propiciando mejora en la economía y en la calidad de vida de su población, y la reducción de su vulnerabilidad al cambio climático.

MISIÓN

Ejecutar y promover los instrumentos de política forestal nacional, facilitando el acceso a los servicios forestales que presta la institución a los actores del sector forestal, mediante el diseño e impulso de programas, estrategias y acciones que generen un mayor desarrollo económico, ambiental y social del país.



Instituto Nacional de Bosques
más bosques. más vida

Plan de Continuidad de Tecnologías de la Información
Unidad de Tecnologías de la Información y Comunicación

I.	INTRODUCCIÓN	3
II.	OBJETIVOS.....	3
III.	ALCANCE	3
IV.	RESPONSABLE	3
V.	TÉRMINOS Y DEFINICIONES.....	3
VI.	DESCRIPCIÓN DEL PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN.....	4
6.1	ANÁLISIS DE RIESGOS Y VULNERABILIDADES.....	4
6.1.1	Identificación de riesgos y amenazas, evaluación y clasificación.....	4
6.2	ESTRATEGIAS DE CONTINUIDAD	5
6.2.1	Planes de respuesta a diferentes escenarios de interrupción	5
6.3	PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍAS DE LA INFORMACIÓN.....	7
6.4	RECURSOS NECESARIOS PARA RECUPERACIÓN.....	10
6.5	INFRAESTRUCTURA TECNOLÓGICA.....	10
6.6	RECURSOS HUMANOS	11
6.6.1	Políticas para el personal durante una crisis.....	11
6.6.2	Procedimientos de notificación y reubicación del personal.....	11
6.7	SOCIALIZACIÓN Y CONCIENCIACIÓN SOBRE EL PLAN DE CONTINUIDAD.....	11
6.8	COMUNICACIONES	12
6.8.1	Lista de contactos internos y externos	12
6.8.2	Procedimientos de comunicación interna y externa.....	12
6.8.3	Estrategias de comunicación de crisis	12
6.9	PRUEBAS Y EJERCICIOS	12
6.9.1	Planificación de simulacros y ejercicios	12
6.9.2	Evaluación y revisión de resultados.....	12
6.9.3	Actualización del Plan de Continuidad según los hallazgos	13
6.10	MANTENIMIENTO Y REVISIÓN.....	13
6.10.1	Procedimientos para la revisión y actualización regular del Plan de Continuidad. ...	13
VII.	CONTROL DE CAMBIOS	13



Instituto Nacional de Bosques
más bosques, más vida

Plan de Continuidad de Tecnologías de la Información
Unidad de Tecnologías de la Información y Comunicación

I. INTRODUCCIÓN

El Instituto Nacional de Bosques dentro de su Política de Continuidad de Tecnologías de la Información, establece los principios y compromisos que determinan el marco bajo el cual el presente plan debe regirse, de manera que garantice la continuidad de los procesos asociados a las tecnologías de la información.

Este plan se declara de alta importancia en la institución para garantizar la continuidad de las operaciones que se desarrollan en el cumplimiento de la Política de Continuidad de Tecnologías de la Información, Política de Calidad y de la Ley Forestal con sus Reglamentos en vigencia.

II. OBJETIVO

Cumplir con lo establecido por la Política de Continuidad de Tecnologías de la Información del INAB con el fin de prevenir, identificar y eliminar los riesgos de interrupción, así como asegurar las condiciones para la recuperación de las operaciones más críticas de la institución en caso de que ocurran, a través de acciones definidas dentro de este documento.

III. ALCANCE

El alcance del presente plan se circunscribe a los procesos y procedimientos que se desarrollan en toda la institución a nivel nacional que dependan de forma parcial o total del funcionamiento de la Infraestructura de Tecnologías de la Información.

IV. RESPONSABLE

- Jefe (a) de Unidad de Tecnologías de la Información y Comunicación

V. TÉRMINOS Y DEFINICIONES

Término	Definición
Riesgo	Combinación de probabilidad de ocurrencia de un evento de seguridad de la información y su consecuencia.
Amenaza	Causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la organización.

Ataque cibernético	Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de información.
--------------------	---

VI. DESCRIPCIÓN DEL PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

6.1 ANÁLISIS DE RIESGOS Y VULNERABILIDADES

6.1.1 Identificación de riesgos y amenazas, evaluación y clasificación

Considerando que el Centro de Datos del INAB centraliza todos los servicios informáticos para internos y externos, se ha realizado la identificación de los riesgos y amenazas que pueden afectar de forma crítica la continuidad de las operaciones institucionales, así como su probabilidad, su impacto y la clasificación del riesgo según su impacto.

No.	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD	IMPACTO	NIVEL CRÍTICO
1	Servidores de aplicaciones y/o de base datos con motor de base de datos con sistema dañado	3	Parcial	Medio
2	Ataque cibernético a servidores	2	Parcial	Medio
3	Corte de servicio de internet	1	Total	Alto
4	Corte de energía eléctrica	1	Total	Alto

Se ha ordenado la lista de riesgos de los más leves a los más críticos, siendo los de nivel crítico "Medio" aquellos que dependen de procedimientos internos para el restablecimiento de los servicios y su impacto es "Parcial", pues no todos los servicios son afectados; nivel crítico "Alto" son aquellos que su impacto depende de terceros (externos) con quienes se debe dar seguimiento hasta resolver el inconveniente, pero se debe prever con acciones e infraestructura alterna para poder resolver mientras se restablecen los servicios de terceros.

6.2 ESTRATEGIAS DE CONTINUIDAD

6.2.1 Planes de respuesta a diferentes escenarios de interrupción

No.	Descripción del riesgo	Plan de Respuesta	Responsable	Estrategia para minimizar Tiempo de Inactividad	Recuperación Alternativa
1	Servidores de aplicaciones y/o de Base de Datos con Motor de Base de Datos con sistema dañado	1. Comunicación a la Gerencia sobre incidente 2. Restablece nuevo servidor virtual alternativo con las especificaciones técnicas mínimas, con nueva IP interna 3. Inactiva el servidor dañado. 4. Activa nuevo servidor con Nateo hacia los DNS con la IP pública correspondiente 5. Configura la aplicación y/o restaura la última versión según backup, si fuera necesario 6. Pruebas de producción 7. Comunicación de Servidor restablecido.	• Jefe de Tecnologías de Desarrollo de Sistemas y Bases de Datos • Responsable de Infraestructura y telecomunicaciones	➤ Se tiene servidor alternativo ya pre-configurado. ➤ El tiempo de inactividad se ocuparía en colocar la copia de respaldo si fuera necesario, y paralelamente se aplican las políticas en Firewall para nuevo NAT. ➤ Tiempo máximo 1 hora	➤ Servidor previamente configurado con las mismas características disponible por cualquier eventualidad. ➤ Copia de Respaldo
2	Ataque cibernético a servidores	1. Comunicación a la Gerencia sobre incidente 2. Restablece nuevo servidor virtual alternativo con las especificaciones técnicas mínimas, con nueva IP interna 3. Instala los servicios necesarios del sistema operativo del servidor, así como motor de BD cuando corresponda. 4. Inactiva el servidor comprometido.	• Jefe de Tecnologías de Desarrollo de Sistemas y Bases de Datos • Responsable de Infraestructura y telecomunicaciones Resle	➤ Se tiene servidor alternativo ya pre-configurado. ➤ El tiempo de inactividad se ocuparía en aplicar políticas de protección en colocar la copia de respaldo, paralelamente se	➤ Servidor previamente configurado con las mismas características disponible por cualquier eventualidad. ➤ Copia de Respaldo

3	Corte de servicio de Internet	5. Establece políticas de bloqueo del origen del ataque 6. Activa nuevo servidor su Nateo hacia los DNS correspondientes con nueva IP Pública no comprometida. 7. Pruebas de producción 8. Comunicación a la Gerencia sobre Servidor restablecido.		aplican las políticas en Firewall para Nateo hacia nueva IP pública NO comprometida. ➤ Tiempo máximo 30 minutos	
4	Corte de Energía eléctrica	1. Comunicación a la Gerencia sobre incidente. 2. Comunicación con Proveedor de Internet para restablecimiento de servicio en el menor tiempo. 3. Activación automática de servicio de internet alternativo. 4. Pruebas de Navegación, respuestas de registro DNS alternativo. 5. Comunicación a la Gerencia sobre servicios restablecidos.	• Jefe de Tecnologías • Responsable de Infraestructura y telecomunicaciones	➤ Previamente se han configurado todos los registros DNS alternos, así como las políticas de Nateo en firewall con respuesta a IP públicas de servicio redundante ➤ Configuración Activo de servicio alternativo ➤ Tiempo máximo 30 minutos (tiempo de pruebas)	➤ Servicio de Internet redundante activo
		1. Comunicación a Gerencia sobre incidente. 2. Comunicación con Proveedor de electricidad para el restablecimiento del servicio en el menor tiempo. 3. Activación automática de servicio eléctrico alternativo (Planta eléctrica).	• Jefe de Tecnologías • Responsable de Infraestructura y telecomunicaciones	➤ UPS del Centro de Datos Funcionado para garantizar el bypass entre servicio primario y alternativo sin corte de alimentación para equipos.	➤ Servicio de Internet redundante activo

		4. Supervisión para abastecimiento de combustible según el periodo del corte. 5. Comunicación a la Gerencia sobre mantenimiento de servicios mientras se establece el retorno de energía eléctrica primaria.		➤ Configuración previa de bypass automático para que servicio alterno comience a trabajar después de los 15 segundos de corte de energía primaria.	
--	--	--	--	---	--

6.3 PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍAS DE LA INFORMACIÓN

Se ha identificado dos sucesos críticos los cuales pueden detener las operaciones de la Institución en un tiempo muy prolongado si no se atienden de forma planificada, a continuación, se establece el plan de respuesta ante estos posibles eventos:

No.	DESCRIPCIÓN DEL RIESGO	Plan de Respuesta	Responsable	Estrategia para minimizar Tiempo de Inactividad	Recuperación Alternativa
1	Intrusión física al Centro de datos para provocar daños a la infraestructura del Centro de Datos	1. Comunicación a Gerencia sobre incidente. 2. Comunicación con Servicios Generales para acciones sobre seguridad en el Centro de Datos. 3. Comunicación a Autoridades competentes por posible hecho delictivo. 4. Comunicación con la Dirección de Asuntos Jurídicos para acciones legales. 5. Comunicación con la Unidad de Comunicación Social para manejo de Medios.	- Gerencia - Jefe Comunicación Social - Jefe de Unidad de Tecnologías - Directores Nacionales, Regionales, Subregionales - Responsable de Infraestructura y Telecomunicaciones. - Profesional de Desarrollo de Sistemas y Bases de Datos	➤ Sitio Alterno Pre-configurado ➤ Copias de Respaldo en sitio Alterno totalmente probados	➤ Sitio Alterno con todos los servidores de aplicaciones y base de datos alterno

		6. Comunicación de Directores Nacionales, Regionales y Subregionales con Usuarios externos. 7. Establecimiento Temporal de Personal de la Unidad de Tecnologías en Edificio de Dirección Nacional para atender emergencia e iniciar recuperación ante desastres. 8. Activación de servidores en sitio alternativo, el cual puede ser físico o en la nube. 9. Restablecimiento de Backup del sitio alternativo, (dispositivo físico o en la nube) 10. Restablecimiento de todos los servicios desde sitio alternativo (físico en la nube) 11. Comunicación a todos los usuarios internos y externos sobre el restablecimiento de los servicios.	• Técnico III de Soporte • Técnico III de Infraestructura y Telecomunicaciones		
2	Destrucción parcial o total del Centro de datos por cualquier desastre natural o similar.	1. Comunicación a Gerencia sobre incidente y posibles daños al a infraestructura. 2. Comunicación con Servicios Generales para acciones sobre seguridad en el Centro de Datos. 3. Comunicación con la Unidad de Comunicación Social para manejo de Medios. 4. Comunicación de Directores Nacionales, Regionales y Subregionales con Usuarios externos.	• Gerencia • Jefe Comunicación Social • Jefe de Unidad de Tecnologías • Directores Nacionales, Regionales, Subregionales • Responsable de Infraestructura y Telecomunicaciones.	➤ Sitio Alterno Pre-configurado ➤ Copias de Respaldo en sitio Alterno totalmente probados	➤ Sitio Alterno con todos los servidores de aplicaciones y base de datos alternativo

	5. Establecimiento Temporal de Personal de la Unidad de Tecnologías en Edificio de Dirección Nacional para atender emergencia e iniciar recuperación ante desastres. 6. Activación de servidores en sitio alternativo, el cual puede ser físico o en la nube. 7. Restablecimiento de Backup del sitio alternativo, (dispositivo físico o en la nube) 8. Restablecimiento de todos los servicios desde sitio alternativo (físico en la nube) 9. Comunicación a todos los usuarios internos y externos sobre el restablecimiento de los servicios.	• Profesional de Desarrollo de Sistemas y Bases de Datos • Técnico III de Soporte • Técnico III de Infraestructura y Telecomunicaciones	
--	---	---	--

6.4 RECURSOS NECESARIOS PARA RECUPERACIÓN

Para el cumplimiento del Plan de Recuperación es importante contar con:

- a) Sitio Seguro para resguardo de unidad de almacenamiento físico, fuera del centro de datos con doble factor de seguridad de acceso.
- b) Sitio alternativo para resguardo de copias de respaldo, y estas a su vez dentro del sitio alternativo posea opción de respaldo, como doble factor de respaldo.
- c) Sitio alternativo de los servidores más críticos (aplicaciones y bases de datos) con la capacidad de contener las mismas capacidades instaladas en el centro de datos.

Importante:

El presente Plan de recuperación ante desastres es aplicable si se tienen los recursos requeridos para el efecto, el poseer dichos recursos depende totalmente de la disponibilidad financiera de la cual no depende de la Institución si no de los recursos asignados en el presupuesto aprobado por el Congreso de la República, pero sobre todo de los aportes asignados durante el período fiscal, por lo que la institución depende de recursos externos para la aplicación de este plan.

6.5 INFRAESTRUCTURA TECNOLÓGICA

Para la recuperación ante desastres debe cumplirse con una serie de acciones necesarias para contar los elementos suficientes para la recuperación.

1. Servidores pre-configurados con las mismas especificaciones de servidores de aplicaciones y base de datos, para alta disponibilidad y atender cualquier fallo de servidores en producción.
2. Condiciones de Copias de Respaldo
 - a. Plan Anual de Copias de respaldo previamente con proceso de restauración al menos dos veces al mes
 - b. Las copias de respaldo se obtienen desde cada servidor a un servidor de consolidación de backup
 - c. Se realiza restauración de backup dentro de otro servidor (servidor SIFGUA)
 - d. Las copias se extraen a un sitio fuera del espacio físico de servidores con factor de autenticación para su seguridad. (Acceso únicamente para Profesional de Desarrollo de Sistemas y Bases de Datos y Jefe de la Unidad de Tecnologías.
3. Para el caso de daños en la Infraestructura física del Centro de datos tales como Switches, Servidores, SAN y otros, se debe trasladar la solicitud de adquisición de



Instituto Nacional de Bosques
más bosques, más vida

bienes con la Dirección Administrativa y Financiera para gestión de compra, según disponibilidad financiera.

6.6 RECURSOS HUMANOS

6.6.1 Políticas para el personal durante una crisis

El personal de la Unidad de Tecnologías debe apoyar al personal responsable en la implementación del Plan de Continuidad y Plan de Recuperación ante desastres de Tecnologías de la Información del INAB por medio de:

- a. Traslado de equipo del centro de datos a otra ubicación
- b. Atención, comunicación y seguimiento a oficinas remotas
- c. Instalación de cableado estructurado
- d. Instalación de equipo del centro de datos
- e. Turnos de ser necesario 24 x7 hasta restablecer los servicios.

Personal de Direcciones Nacionales, Regionales, Subregionales y Jefes de Unidad

- a. Comunicación Interna a los subalternos para socializar a los usuarios externos sobre las acciones del plan de contingencia para el restablecimiento de los servicios.
- b. Dar el acompañamiento al Usuario para solventar requerimientos en sus servicios

6.6.2 Procedimientos de notificación y reubicación del personal

La reubicación de personal se realizará de acuerdo al lugar donde la Gerencia determine para que el personal de la Unidad de Tecnologías desarrolle el plan de Recuperación.

6.7 SOCIALIZACIÓN Y CONCIENCIACIÓN SOBRE EL PLAN DE CONTINUIDAD

Al menos una vez al año se realizará capacitación a todo el personal de la institución de las políticas y planes de continuidad y Recuperación para su conocimiento a través del Departamento de Formación de Personal.

6.8 COMUNICACIONES

6.8.1 Lista de contactos internos y externos

La Unidad de Tecnologías tendrá la actualización de contactos Internos (correos y teléfonos) a nivel nacional para las diferentes comunicaciones oficiales, las cuales se realizarán en las diversas plataformas de comunicación.

La lista de contactos Externos estará a cargo de cada administrador de sistemas, quienes mantendrán las comunicaciones con sus usuarios por medio de las Regiones y Subregiones.

6.8.2 Procedimientos de comunicación interna y externa

Las comunicaciones se realizarán de acuerdo a la urgencia del evento.

- Por Correo por medio de la plataforma INFO-INAB a usuarios internos y externos
- Por Teléfono, todas las comunicaciones de emergencia.

6.8.3 Estrategias de comunicación de crisis

Las comunicaciones en caso de crisis serán dirigidas por la Unidad de Comunicación Social quien establecerá la estrategia de comunicación según sea el caso de la crisis, por lo que toda comunicación oficial deberá ser atendida por dicha unidad previamente autorizada por la Gerencia.

6.9 PRUEBAS Y EJERCICIOS

6.9.1 Planificación de simulacros y ejercicios

Se realizarán Simulacros replicando incidentes una vez al año por tipo de riesgo, en el segundo cuatrimestre.

6.9.2 Evaluación y revisión de resultados

Se realizará un informe con los resultados del simulacro, se deben registrar los aciertos y desaciertos en la implementación del Plan de Continuidad, y al final del informe se deben dar los resultados finales de la evaluación.



Instituto Nacional de Bosques
Más bosques. Más vida

6.9.3 Actualización del Plan de Continuidad según los hallazgos

Con el Informe de Resultados, de ser necesario se deben realizar las actualizaciones a los Planes, Políticas e inclusive al Manual de Normas, procesos y procedimientos de la Unidad de Tecnologías de la Información.

6.10 MANTENIMIENTO Y REVISIÓN

6.10.1 Procedimientos para la revisión y actualización regular del Plan de Continuidad.

- La Unidad de Tecnologías realizará las actualizaciones necesarias al Plan de Continuidad como parte de la mejora continua.
- El plan deberá ser trasladado al Departamento de Gestión de la Calidad para su revisión y posterior traslado a Gerencia, para su autorización.

VII. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión actualizada	Descripción del cambio	Fecha de aprobación del cambio
	N/A	