***Aprobado por la Dirección Ejecutiva el 30 de agosto 2021***



**OFICINA NACIONAL DE SEMILLAS**

**PLAN DE CONTINUIDAD DE SERVICIOS
DE TECNOLOGÍA DE INFORMACIÓN**

# CONTENIDO

[CONTENIDO 1](#_Toc80714354)

[PLAN DE CONTINGENCIA 3](#_Toc80714355)

[INTRODUCCION 4](#_Toc80714356)

[OBJETIVO PRINCIPAL 5](#_Toc80714357)

[OBJETIVOS ESPECIFICOS 5](#_Toc80714358)

[ALCANCE 5](#_Toc80714359)

[DEFINICIONES 5](#_Toc80714360)

[EQUIPOS DE TRABAJO 6](#_Toc80714361)

[DATOS INFORMATIVOS 7](#_Toc80714362)

[ANALISIS DE IMPACTO DE LOS PROCESOS 9](#_Toc80714363)

[METODOLOGIA DE TRABAJO 10](#_Toc80714364)

[DEFINICIONES DE TERMINOS 10](#_Toc80714365)

[ANALISIS Y EVALUACION DE RIESGOS 11](#_Toc80714366)

[ESCENARIOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA 12](#_Toc80714367)

[PLANIFICACIÓN 13](#_Toc80714368)

[DISEÑO DE ESTRATEGIA DE CONTINUIDAD DE LOS PROCESOS Y SERVICIOS QUE BRINDA LA OFICINA NACIONAL DE SEMILLAS 13](#_Toc80714369)

[FALLA EN EQUIPO TERMINAL. 14](#_Toc80714370)

[FALLA EN EL SERVIDOR PRINCIPAL (CRÍTICO). 16](#_Toc80714371)

[INTERRUPCIÓN DEL SERVICIO DE INTERNET 19](#_Toc80714372)

[INTERRUPCIÓN DEL FLUIDO ELÉCTRICO 20](#_Toc80714373)

[INDISPONIBILIDAD DE LA CENTRAL TELEFONICA 21](#_Toc80714374)

[INDISPONIBILIDAD DE LA PAGINA WEB DE LA OFICINA NACIONAL DE SEMILLAS 22](#_Toc80714375)

[INDISPONIBILIDAD DE SISTEMA DE REGISTROS (USUARIOS, IMPORTACIONES, EXPORTACIONES). 23](#_Toc80714376)

[INDISPONIBILIDAD DE SISTEMA DE REGISTROS VARIEDADES COMERCIALES. 25](#_Toc80714377)

[INDISPONIBILIDAD DE SISTEMA DE SEGUIMIENTO DE ACTIVIDADES DE CERTIFICACION Y CONTROL DE CALIDAD DE SEMILLAS (SACCS). 26](#_Toc80714378)

[INDISPONIBILIDAD DE SISTEMA DE ADMINISTRATIVO CONTABLE (ERP\_CONSULTANTS). 28](#_Toc80714379)

[INDISPONIBILIDAD DEL CENTRO DE CÓMPUTO 29](#_Toc80714380)

[AUSENCIA PARCIAL O PERMANTE DEL PERSONAL DE TI. 31](#_Toc80714381)

[PLAN DE VERIFICACION Y PRUEBAS 31](#_Toc80714382)

[PLAN DE VERIFICACIÓN 32](#_Toc80714383)

[PROCEDIMIENTO PARA LAS PRUEBAS DEL PLAN DE CONTINGENCIA 32](#_Toc80714384)

[OBJETIVO 32](#_Toc80714385)

[MÉTODOS DE PRUEBAS DE CONTINGENCIA 33](#_Toc80714386)

[ANEXOS 35](#_Toc80714387)

[LISTADO DE PROVEEDORES DE SERVICIOS Y CONTACTOS. 35](#_Toc80714388)

# PLAN DE CONTINGENCIA

Para la Oficina Nacional de Semillas es indispensable recurrir a los recursos de Tecnologías de la Información y Comunicaciones (TICs) como un medio para proporcionar los servicios que la oficina ofrece a sus usuarios y es de vital importancia que dicha información este a la mano para poder brindar sus servicios.

Es importante resaltar que para la Oficina Nacional de Semillas logre sus objetivos necesita garantizar tiempos de indisponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones; de este modo podrá garantizar la atención a los usuarios internos en todas las áreas operativas.

Por todo lo mencionado anteriormente, el estar sin el servicio de la plataforma informática por un lapso mayor de 4 horas origina distorsiones al funcionamiento normal de nuestros servicios. De continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar las operaciones de los clientes en sus importaciones y exportaciones, entre otros servicios que brinda la Oficina.

Es necesario, por tanto, prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo menor posible.

#

# INTRODUCCION

El presente documento es el Plan de Contingencia Informático del Oficina Nacional de Semillas de Acceso a la Información en materia de Riesgos de Tecnología de Información y Comunicaciones (TIC).

Establece el objetivo, alcance y metodología desarrollada. Incluye además, las definiciones utilizadas, las políticas de seguridad, el análisis de la situación, el análisis de sensibilidad de la información manejada, la identificación de los riesgos y controles, y la clasificación de activos de TIC.

La metodología práctica comprende: la identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.

Permitirá mantener la contingencia operativa frente a eventos críticos de la Oficina Nacional de Semillas y minimizar el impacto negativo sobre el mismo, los usuarios deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

Ha sido elaborado tomando como base, la Metodología ITIL (INFORMATION TECNOLOGY INFRASTRUCTURE LIBRARY).

#

# OBJETIVO PRINCIPAL

Establecer el procedimiento a seguir en caso de presentarse una contingencia en los servicios críticos de TI, con el fin de mitigar los riegos, minimizar pérdidas en la Institución y brindar una continuidad del negocio.

# OBJETIVOS ESPECIFICOS

* Mantener el nivel de servicio en límites predefinidos.
* Establecer un periodo de recuperación.
* Determinar la capacidad que puede tener la institución en caso de materializarse un riesgo de alto impacto.
* Mitigar permanentemente el riesgo de interrupción de servicios.
* En caso de crisis garantizar un efectivo flujo de las comunicaciones internas y externas.
* Garantizar en principio la recuperación de la operación crítica en el menor tiempo posible.

# ALCANCE

El alcance de este documento es brindar al personal de la Oficina Nacional de Semillas las directrices a seguir en caso de una contingencia en los servicios críticos de TI y los responsables de cada actividad.

# DEFINICIONES

1. **CONTINGENCIA:**

Interrupción, no planificada, de la disponibilidad de recursos informáticos.

1. **PLAN DE CONTINGENCIA:**

Conjunto de medidas (de DETECCION y de REACCION) a poner en marcha ante la presentación de una contingencia.

El Plan de Contingencia se subdivide en:

* + 1. Plan de Emergencia
		2. Plan de Restauración (BACKUP)
		3. Plan de Recuperación

El Plan de Contingencia suele combinarse con planes de seguridad general.

1. **PLANES:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **EMERGENCIA** | **RESTAURACION** | **RECUPERACION** |
| **OBJETIVO** | Limitar el daño. | Continuar Procesos Vitales. | Recuperar proceso total. |
| **ACTUACION** | Inmediata. | A Corto Plazo (Máximo 24 horas). | A Mediano Plazo (Máximo 48) |
| **CONTENIDO** | Evacuación.Valoración de Daños.Arranque de acciones. | Alternativas para los Procesos vitales.  | Estrategias para la recuperación de todos los recursos. |
| **RESPONSABILIDAD** | Oficina Nacional de Semillas. | Usuarios. | Encargado de Sistemas. |

#

# EQUIPOS DE TRABAJO

Los equipos de trabajo, sus actividades e integrantes están conformados según el siguiente cuadro:

|  |  |  |
| --- | --- | --- |
| **Equipos** | **Funciones** | **Integrantes** |
|  | Dirigir las actividades durante la contingencia y recuperación.* Análisis de la situación
* Activación o no del plan de recuperación
* Seguimiento del proceso de recuperación
* Evaluación de los daños
 | Encargados de TI |
|  | Jefatura Administrativa |
| Equipo Director | Jefatura Técnica |
|  | Dirección Ejecutiva |
| Equipo de Logística | Proveerá la logística necesaria para las actividades de recuperación:* Contacto con los proveedores
* Compra de Equipos
 | Encargados de TI |
| Equipo deRecuperación | Restablecer todos los servicios principales de TI que son:* Servidor Principal
* Servidores Virtuales
* Sistema de Información (Sistema Contable, Sistema de Registros de Importación y Exportación, sistema de Variedades Comerciales,
* Página Web de la Institución.
 | Jefe Departamento Administrativo |
| Equipo de Pruebas | Realizarán las pruebas de verificación de operación de los servicios principales de TI. | Encargados de TI Funcionarios de la O.N.S |

#

# DATOS INFORMATIVOS

A continuación se coloca la información de contacto de miembros de equipos, proveedores, centros alternos y líderes de área.

|  |
| --- |
| **EQUIPO: SISTEMAS** |
| **DATOS** | **LIDER** | **SUPLENTE** |
| Nombre | José Rodríguez Molina | Roger Valverde Rovira |
| Cargo | Encargado de TI | Desarrollador de Sistemas. |
| Celular  | 8816-4593 | 8405-6668 |
| Teléfono  | 2223-5922 EXT 115 | 2223-5922 EXT 120 |
| Correo | jrodriguez@ofinase.go.cr | rvalverde@ofinase.go.cr |

# ANALISIS DE IMPACTO DE LOS PROCESOS

**Objetivo Principal:**

El objetivo principal del Análisis del Impacto de los procesos, es determinar las funciones, procesos e infraestructura de soporte que son críticos para la contingencia operativa de la Oficina Nacional de Semillas.

**Objetivos Específicos:**

Para lograr el objetivo principal se definieron los siguientes objetivos específicos:

1. Identificar las preocupaciones y prioridades de que deberá asumir la Oficina Nacional de Semillas en el caso que exista una indisponibilidad en los sistemas informáticos producida por una contingencia.
2. Identificar el tiempo máximo en el que un proceso crítico de los sistemas de información deberá ser restaurado para su normal y eficiente continuidad.
3. Identificar el impacto en las aplicaciones que soportan los procesos críticos.
4. Proporcionar las bases de una estrategia para la contingencia operativa en caso de un desastre.

Principales Procesos Identificados:

1. **SERVIDORES:**
	1. Servidor Físico Principal.
	2. Servidores Virtuales:
		1. Servidor de Dominio
		2. Servidor de Base de Datos.
		3. Servidor de Archivos.
	3. Servidor físico de Firewall
		1. Servidor Firewall .
2. **SOFTWARE:**
* Sistema de Control de Registros de Importación y Exportación.
* Sistema de Registro de Variedades.
* Sistema Contable (ERP Consultants).
* Sistema de Seguimiento de Actividades de Certificación y Control de Calidad de Semillas.
* Página Web.
* Sistema de Contable de ASOFINASE (ASODATA).
1. **SOFTWARE BASE DE DATOS**:
* Base de Datos SQL Server
	+ ASODATA
	+ ASODATA\_AUDITORIA
	+ Bit2
	+ ONS\_Seguridad
	+ Reloj\_3210
	+ SAAE
	+ SAAE\_AUDITORIA
	+ SACCS

#  METODOLOGIA DE TRABAJO

El Análisis del Impacto tiene como objetivo determinar los procesos críticos y las aplicaciones que lo soportan con el fin de proporcionar las bases para el Plan de Recuperación de TI.

Se llevarán a cabo las siguientes actividades:

a) Entrevistas a diferentes funcionarios responsables de las distintas áreas.

b) División de los procesos en líneas:

i) Identificación de los Procesos

ii) Subprocesos

iii) Aplicaciones que soporta la Oficina Nacional de Semillas.

iv) Máximo tiempo de interrupción en que el subproceso puede estar interrumpido en horas.

c) Validación de la criticidad por proceso.

# DEFINICIONES DE TERMINOS

Para la mejor comprensión de los términos y contenido de este plan, se detallan las siguientes definiciones:

**Proceso crítico:** Proceso considerado indispensable para la continuidad de las operaciones y servicios de la Oficina Nacional de Semillas, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución.

* **Impacto:** El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos TI, en:
	+ **Impacto Alto:** Se considera que una actividad crítica tiene impacto alto sobre las operaciones de la institución, cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente.
	+ **Impacto Medio:** Se considera que una actividad crítica tiene un impacto medio cuando la falla de ésta ocasiona una interrupción en las operaciones por un tiempo mínimo de tolerancia.
	+ **Impacto Bajo:** Se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta, no tiene un impacto en la continuidad de las operaciones de la institución.
* **Plan de Contingencia:**
	+ Son procedimientos que definen cómo un negocio continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
	+ Los sistemas de TI son vulnerables a diversas interrupciones.
		- **Leves:** Caídas de energía de corta duración, fallas en disco duro, etc.
		- **Severa:** Destrucción de equipos, incendios, etc.
	+ Asegura que se dé una interrupción mínima a los procesos de negocios en caso de una interrupción significativa de los servicios que normalmente soportan esos procesos.
	+ Todos los aplicativos críticos y sistemas de soporte general deben tener un plan de contingencias.

# ANALISIS Y EVALUACION DE RIESGOS

Los desastres causados por un evento natural o humano, pueden ocurrir, en cualquier parte, hora y lugar. Existen distintos tipos de Riesgos:

* **Riesgos Naturales:** tales como mal tiempo, terremotos, etc.
* **Riesgos Tecnológicos:** tales como incendios eléctricos, fallas de energía, accidentes de transmisión, transporte de activos, ataques a servidores y robo de información.
* **Riesgos Sociales:** como actos terroristas y desordenes.
* **Riegos Institucionales:** como falta de usuario experto, presupuesto para compras de equipo, mantenimiento de equipos, etc.

Las causas más representativas que originarían cada uno de los escenarios propuestos en el Plan de Contingencias y Seguridad de la Información se presentan en el siguiente cuadro:

|  |  |
| --- | --- |
| **CAUSAS** | **ESCENARIOS** |
| * Falla Corte de Cable UTP.
* Falla Tarjeta de Red.
* Falla IP asignado.
* Falla Punto de Switch.
* Falla Punto Patch Panel.
* Falla Punto de Red.
* Falla en Memoria Ram.
* Falla en Disco Duro.
* Falla en Fuente de Poder.
* Falla en Tarjeta de Video.
* Falla en Tarjeta Madre.
 | 1. FALLA EN EQUIPO TERMINAL.
 |
| * Fallas de Componentes de Hardware del Servidor.
* Fallas de Software del Servidor.
* Falla del UPS (Falta de Suministro eléctrico).
* Virus.
* Sobrepasar el límite de almacenamiento del Disco.
* Fallas en Discos Duros del Servidor.
 | 1. FALLA EN SERVIDOR.
 |
| * Falla de equipos de comunicación: SWITCH, Fibra Óptica.
* Fallas en el software de Acceso a Internet.
* Perdida de comunicación con proveedores de Internet.
 | 1. PERDIDA DE SERVICIO DE INTERNET.
 |
| * Corte General del Fluido eléctrico interno.
* Corte General del Fluido eléctrico interno.
* Falta de pago de servicio eléctrico.
 | 1. INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.
 |
| * Fallo en la central telefónica (Por software o Hardware),
* Fallo en la configuración de la central telefónica.
* Fallo en terminal de teléfono.
 | 1. INDISPONIBILIDAD DE LA TELEFONIA IP.
 |
| * Falla en el servidor web del proveedor.
* Falla en la publicación de la página web de la oficina.
* Falla por bloqueos de seguridad.
 | 1. INDISPONIBILIDAD DE LA PÁGINA WEB DE LA OFICINA NACIONAL DE SEMILLAS
 |
| * Fallo en acceso al sistema.
* Fallo en la funcionalidad del sistema.
* Fallo en componentes del sistema por actualizaciones.
* Fallo en la tablas de base de datos (Corruptas .dbf)
 | 1. INDISPONIBILIDAD DE SISTEMA DE REGISTROS.DE USUARIOS, IMPORTACIONES Y EXPORTACIONES.
 |
| * Fallo en acceso al sistema.
* Fallo en la funcionalidad del sistema.
* Fallo en componentes del sistema por actualizaciones.
* Fallo en la tablas de base de datos (Corruptas .dbf)
 | 1. INDISPONIBILIDAD DE SISTEMA DE REGISTROS.DE VARIEDADES COMERCIALES
 |
| * Fallo en acceso al sistema.
* Fallo en acceso a la base de datos del sistema.
* Fallo en la funcionalidad del sistema.
* Fallo en componentes del sistema por actualizaciones.
 | 1. INDISPONIBILIAD DE SISTEMA DE SEGUIMIENTO DE ACTIVIDADES DE CERTIFICACION Y CONTROL DE SEMILLAS (SACCS).
 |
| * Fallo en acceso al sistema.
* Fallo en acceso a la base de datos del sistema.
* Fallo en la funcionalidad del sistema.
* Fallo en componentes del sistema por actualizaciones.
 | 1. INDISPONIBILIDAD DE SISTEMA ADMINISTRATIVO CONTABLE (ERP CONSULTANTS)
 |
| * Incendio
* Sabotaje
* Corto Circuito
* Terremoto
 | 1. INDISPONIBILIDAD DEL CENTRO DE CÓMPUTO (DESTRUCCIÓN DEL SITIO DE SERVIDORES)
 |
| * Accidente.
* Incapacidad.
* Vacaciones.
* Renuncia Intempestiva
 | 1. AUSENCIA PARCIAL O PERMANENTE DEL

PERSONAL DE TECNOLOGÍA DE LAINFORMACIÓN. |

##

## ESCENARIOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA

1. FALLA EN EQUIPO TERMINAL.
2. FALLA EN SERVIDOR.
3. PERDIDA DE SERVICIO DE INTERNET.
4. INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.
5. INDISPONIBILIDAD DE LA TELEFONIA IP.
6. INDISPONIBILIDAD DE LA PÁGINA WEB DE LA OFICINA NACIONAL DE SEMILLAS.
7. INDISPONIBILIDAD DE SISTEMA DE REGISTROS.DE USUARIOS, IMPORTACIONES Y EXPORTACIONES.
8. INDISPONIBILIDAD DE SISTEMA DE REGISTROS.DE VARIEDADES COMERCIALES.
9. INDISPONIBILIAD DE SISTEMA DE SEGUIMIENTO DE ACTIVIDADES DE CERTIFICACION Y CONTROL DE CALIDAD DE SEMILLAS (SACCS).
10. INDISPONIBILIDAD DE SISTEMA ADMINISTRATIVO CONTABLE (ERP CONSULTANTS).
11. INDISPONIBILIDAD DEL CENTRO DE CÓMPUTO.
12. AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE SISTEMAS INFORMÁTICOS.

La evaluación y administración de estos riesgos que van a permitir a la Oficina Nacional de Semillas:

* Desarrollar estrategias de recuperación y respaldo de las decisiones operacionales, tecnológicas y humanas.
* Identificar los controles existentes y los nuevos controles a implementar para minimizar los riesgos, evaluando el costo / beneficio de dichos controles.
* Planificar la seguridad de la información.

## PLANIFICACIÓN

* Tiempo máximo de la contingencia.
* Costos estimados.
* Recursos humanos.
* Capacitación.
* Retorno a la normalidad.
* Validar el plan de contingencia

#

# DISEÑO DE ESTRATEGIA DE CONTINUIDAD DE LOS PROCESOS Y SERVICIOS QUE BRINDA LA OFICINA NACIONAL DE SEMILLAS

1. **Estrategia de Respaldo y Recuperación**
	1. Planificar la necesidad de personal adicional para atender las necesidades conforme a las necesidades de la Oficina Nacional de Semillas.
	2. Planificar el cierre y reinicio progresivo de los dispositivos y sistemas que se consideran en riesgo.
2. **Almacenamiento y Respaldo de la Información (BACKUPS)**
	1. Los Backup de las base de datos y de la información se realizan (diario o periódico, incremental o total) considerando la criticidad de los datos y la frecuencia con que se introduce nueva información.
	2. Los datos se respaldaran en discos magnéticos o discos ópticos con una rotación de los disco por semana.
	3. Los respaldos se guardan como sitio alternativo externo para el almacenamiento de la información más importante en la nube.
3. **Roles y Responsabilidades**
	1. El encargado de TI es el responsable de la implementación del plan y toma de decisiones al momento de un fallo en los servicios de la Oficina Nacional de Semillas.
	2. El personal de la recuperación se asignará a equipos específicos que responderán al evento, recuperarán los sistemas de TI y restaurarán operaciones normales.
	3. Los tipos específicos de equipos requeridos dependen del sistema afectado.
4. **Tipos de Equipos**
	1. Gestión de la crisis: El responsable de este equipo será el administrador, el cual tendrá que reportar directamente con el encargado de la crisis.
	2. Evaluación de daños: estará a cargo de especialistas auditoría interna, encargado de TI y cualquier otro personal que crea conveniente incluir.
	3. Ellos determinarán la magnitud de todos los posibles daños que hayan ocurrido durante una contingencia.
	4. Recuperación de sistemas operativos, utilitarios, servidores, redes, bases de datos, aplicaciones y telecomunicaciones: este equipo estará formado por personal de sistemas de la institución.
	5. Prueba del plan: El encargado de este equipo será personal de sistemas de la institución.
	6. Compras (equipos y suministros): este equipo estará conformado por personal de logística, encargado de sistemas y el jefe administrativo de la institución. El Jefe Administrativo señalará a las personas adecuadas para este equipo.

 **Consideraciones de Costos**

* Asegurar que la estrategia elegida pueda implementarse de manera eficaz con el personal y recursos financieros disponibles.
* Determinar un presupuesto de gastos para el planeamiento de contingencias:
	+ Software y hardware.
	+ Transporte.
	+ Pruebas.
	+ Entrenamiento.
	+ Materiales.
	+ Tiempo a incurrir.
	+ Servicios.

## FALLA EN EQUIPO TERMINAL.

**Impacto**

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| No se puede trabajar con el equipo asignado | Área en que labora. |
| Problemas de comunicación en la red | Área en que labora. |
| Interrupción de sus actividades propias. | Área en que labora. |

**Tiempos aceptables de caída.**

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO HORAS** |
| 1. Problemas de Hardware | ALTO | 24 |
| 2. Problemas de Software | ALTO | 24 |

Causas de las fallas en el equipo terminal.

* Falla Corte de Cable UTP.
	+ En este caso se dan los siguientes síntomas:
		- Falta de comunicación en la red y el equipo de reciba o envié datos.
* Falla Tarjeta de Red.
	+ En este caso se dan los siguientes síntomas:
		- Falta de comunicación en la red y el equipo de reciba o envié datos.
* Falla IP asignado.
	+ En este caso se dan los siguientes síntomas:
		- No se puede acceder a la red por conflicto de IP con otro equipo.
* Falla Punto de Switch.
	+ En este caso se dan los siguientes síntomas:
		- Falta de comunicación en la red y el equipo de reciba o envié datos.
* Falla Punto Patch Panel.
	+ En este caso se dan los siguientes síntomas:
		- Falta de comunicación en la red y el equipo de reciba o envié datos.
* Falla Punto de Red.
	+ En este caso se dan los siguientes síntomas:
		- Falta de comunicación en la red y el equipo de reciba o envié datos.
* Falla en Memoria Ram.
	+ En este caso se dan los siguientes síntomas:
		- Equipo enciende pero no da video.
		- Equipo enciende y hace indicación de fallo en memoria ram por medio de un pito constante.
* Falla en Disco Duro.
	+ En este caso se dan los siguientes síntomas:
		- Equipo no encuentra disco duro en BIOS.
		- No inicia el sistema operativo con normalidad.
* Falla en Fuente de Poder.
	+ En este caso se dan los siguientes síntomas:
		- Equipo no enciende.
* Falla en Tarjeta de Video.
	+ En este caso se dan los siguientes síntomas:
		- Equipo enciende y no muestra imagen en monitor del BIOS o del sistema operativo.
* Falla en Tarjeta Madre.
	+ En este caso se dan los siguientes síntomas:
		- Equipo enciende pero no da funcionalidad no mostrando imagen en el monitor.

Recursos de Contingencia

* En caso de que el equipo terminal cuente con garantía debe ser llevado al proveedor para su revisión y solución.
* La oficina Nacional de Semillas cuenta equipos de respaldo para que si una computadora falla y no tiene solución inmediata puede ser cambiada, para que el usuario pueda continuar con sus funciones.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

##

## FALLA EN EL SERVIDOR PRINCIPAL (CRÍTICO).

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Paralización de los sistemas o aplicaciones que se encuentran en el servidor que presentan fallas. | Todas las áreas |
| Posible Pérdida de Hardware y Software. | Área de TI |
| Perdida del proceso automático de Backup | Área de TI |
| Interrupción de las operaciones | Área de TI |

Tiempos aceptables de Caída.

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO HORAS** |
| 1. Servidor Base de Datos | ALTO | 24 |
| 2. Servidor de Archivos – Aplicaciones. | ALTO | 24 |
| 3. Servidor de Controlador de Dominio Primario | ALTO | 24 |
| 4. Servidor FIREWALL  | ALTO | 24 |

**Causas de la Falla del Servidor.**

* **Error Físico de Disco de un Servidor.**
	+ Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:
		- Ubicar el disco dañado.
		- Realizar solicitud de Compra de parte requerida.
		- Realizar sustitución de disco dañado.
		- Realizar reparación de arreglo de discos para que entre en funcionamiento.
		- Verificar que el disco funcione correctamente.
		- Verificar que no se presente ninguna afectación en servicios del servidor.
* **Error de Memoria RAM**
	+ En este caso se dan los siguientes síntomas:
		- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
		- Ante procesos mayores se congela el proceso.
		- Arroja errores con mapas de direcciones hexadecimales.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la institución, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias dañadas.
4. Retirar las memorias dañadas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.

Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

* **Error de Tarjeta(s) Controladora(s) de Disco**

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

* 1. Avisar a los usuarios que deben salir del sistema.
	2. El servidor debe estar apagado, dando un correcto apagado del sistema.
	3. Ubicar la posición de la tarjeta controladora.
	4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
	5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
	6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
	7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.
* **Error Lógico de Datos**

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

* 1. Caída del servidor de archivos por falla de software de red.
	2. Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
	3. Bajar incorrectamente el servidor de archivos.
	4. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

**PASO 1:** Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos.

**PASO 2**: Deshabilitar el ingreso de usuarios al sistema.

**PASO 3:** Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargar también.

**PASO 4:** Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

**PASO 5:** Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

* **Caso de Virus**

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

1. Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación
2. El antivirus muestra el nombre del archivo infectado y quién lo usó.
3. Estos archivos (exe, com, etc),
4. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

 Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

## INTERRUPCIÓN DEL SERVICIO DE INTERNET

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Caída de servicio de Internet por fallas en el centro de comunicaciones. | Todas las áreas |
| Caída del servicio de internet por fallas del proveedor del servicio en la zona.  |
| Corte del servicio de internet por falta de pago del servicio. |

Tiempo aceptable de Caída

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Interrupción del servicio de internet por falla internas | ALTO | 12 |
| 2. Interrupción del servicio de internet por fallas en el proveedor del servicio. | ALTO | 24 |
| 3. Pago de Servicio de Internet. | ALTO | 8 |

**Causas de la Interrupción del Servicio de Internet.**

* Interrupción del servicio de internet por falla internas.
	+ Dado el caso crítico de la interrupción interna del servicio de internet, se debe tomar las acciones siguientes:
		- Realizar un chequeo de los dispositivos de red que se encuentren encendidos (Patch Panel, Switch, Router, Modem).
		- En caso de un daño en alguno de los equipo validar garantía y sino informar al jefe superior para su compra.
* **Interrupción del servicio de internet por falla externa.**
	+ En este caso se dan los siguientes síntomas:
		- No se tenga acceso a internet por medio de un navegador, envió y recepción de correos electrónicos.
		- Se debe llamar al proveer de servicio para verificar la falla en la zona o una atención de parte del proveedor.
* **Interrupción del servicio de internet por falta de pago.**
	+ En este caso se dan los siguientes síntomas:
		- No se tenga acceso a internet por medio de un navegador, envió y recepción de correos electrónicos.
		- Se debe llamar al proveer de servicio para verificar la falla en la zona o una atención de parte del proveedor y verificar el estado de la cuenta del servicio.

**Contingencia**

Actualmente la Oficina Nacional de Semillas cuenta con el servicio de dos proveedores de Internet en donde se tiene una IPs como principal (Fibra Óptica del ICE) por 100 MB, y otra IPs como segundaria (Tigo) por 100 MB.

Cabe mencionar con lo indicado anteriormente la oficina cuenta con un equipo de firewall el cual se encarga de realizar la transferencia de IPs cuando la principal falla. El retorno al servicio de internet principal se restablece de forma automática cuando este este activo.

## INTERRUPCIÓN DEL FLUIDO ELÉCTRICO

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Interrupción de fluido eléctrico por fallas internas. | Todas las Áreas |
| Interrupción de fluido eléctrico por fallas externas. |
| Interrupción de fluido eléctrico por falta de pago del servicio. |

Tiempo aceptable de Caída

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Interrupción de fluido eléctrico por fallas internas. | ALTO | 24 |
| 2. Interrupción de fluido eléctrico por fallas externas. | ALTO | 24 |
| 3. Interrupción de fluido eléctrico por falta de pago de Servicio de electricidad. | ALTO | 8 |
| 4. Recarga de tanque de gas. | ALTO | 8 |

**Causas de la Interrupción del Servicio de Electricidad**.

* **Interrupción del servicio de internet por falla internas**.
	+ Dado el caso crítico de la interrupción interna del servicio de internet, se debe tomar las acciones siguientes:
		- Realizar un chequeo de los dispositivos de red que se encuentren encendidos (Patch Panel, Switch, Router, Modem).
		- En caso de un daño en alguno de los equipo validar garantía y sino informar al jefe superior para su compra.
* **Interrupción del servicio de internet por falla externa.**
	+ En este caso se dan los siguientes síntomas:
		- No se tenga acceso a internet por medio de un navegador, envió y recepción de correos electrónicos.
		- Se debe llamar al proveer de servicio para verificar la falla en la zona o una atención de parte del proveedor.
* **Interrupción del servicio de internet por falta de pago.**
	+ En este caso se dan los siguientes síntomas:
		- No se tenga acceso a internet por medio de un navegador, envió y recepción de correos electrónicos.
		- Se debe llamar al proveer de servicio para verificar la falla en la zona o una atención de parte del proveedor y verificar el estado de la cuenta del servicio.

**Recursos de Contingencia**

Actualmente la Oficina Nacional de Semillas, ha implementado varios mecanismos para la mitigación del riesgo por corte de fluido eléctrico, en donde se indican a continuación:

1. Cada Computadora de usuario tiene una UPS (Batería de Respaldo), en donde tiene un duración aproximada de 10 a 20 minutos, para mantener el equipo encendido.
2. El cuarto de servidor cuentan con su propia UPS (Batería de Respaldo), en donde esta tiene una duración aproximada de 2 horas, logrando mantener las operaciones activas para la continuidad del negocio y la atención de parte del área de TI para proceder con los respaldos de base de datos.
3. El cuarto de telecomunicaciones cuentan con su propia UPS (Batería de Respaldo), en donde esta tiene una duración aproximada de 2 horas, logrando mantener las operaciones activas para la comunicación en las instalaciones de la institución.
4. La Oficina Nacional de Semillas cuenta con una planta eléctrica de Gas, en la cual puede producir a la institución una continuidad del negocio por aproximadamente 24 horas con el tanque de gas llego a su capacidad.

Este último entra a funcionar de forma automática cada vez se presente el corte de corriente,

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

## INDISPONIBILIDAD DE LA CENTRAL TELEFONICA

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Interrupción de fluido eléctrico por fallas internas. | Todas las Áreas |
| Interrupción de fluido eléctrico por fallas externas. |
| Interrupción de fluido eléctrico por falta de pago del servicio. |

Tiempo aceptable de Caída

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Falla en la Central Telefónica. | ALTO | 24 |
| 2. Fallo en la Configuración de la central telefónica. | ALTO | 24 |
| 3. Fallo en terminales Telefónicas. | MEDIO | 24 |

**Causas de falla de central telefónica.**

* **Falla en Central Telefónica.**
	+ Dado el caso de la interrupción o falla en la central telefónica, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo de la central telefónica, que tenga corriente eléctrica, que el Switch tenga este encendido y funcionando.
		- Realizar aviso al proveedor de la central para solicitar soporte técnico.
* **Falla en Configuración de la Central Telefónica.**
	+ Dado el caso de la interrupción o falla en la central telefónica por configuración, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar aviso al proveedor de la central para solicitar soporte técnico.
* **Fallo en terminal telefónico.**
	+ Dado el caso de la interrupción o falla en la central telefónica por configuración, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar aviso al proveedor de la central para solicitar soporte técnico.
		- En caso de que la terminar no tenga reparación se debe realizar la cotización del equipo a reponer.

**Recursos de Contingencia**

Actualmente la Oficina Nacional de Semillas, cuenta con un contrato de manteniendo y soporte por parte de la empresa Emetec Costa Rica, en donde brindan un soporte al equipo de tecnológico de la central telefónica.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

## INDISPONIBILIDAD DE LA PAGINA WEB DE LA OFICINA NACIONAL DE SEMILLAS

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Falla en el Servidor Web del Proveedor. | Todas las ÁreasYClientes Externos. |
| Fallas en la publicación de la página web de la ONS. |
| Fallo por bloqueos de seguridad en el servidor. |

Tiempo aceptable de Caída

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Falla en el Servidor Web del Proveedor. | ALTO | 24 |
| 2. Fallas en la publicación de la página web de la ONS. | ALTO | 24 |
| 3. Fallo por bloqueos de seguridad en el servidor. | ALTO | 24 |

**Causas de falla en la página web de la Oficina Nacional de Semillas.**

* **Falla en el Servidor Web del Proveedor.**
	+ Dado el caso de la interrupción o falla en el servidor web del proveedor de servicio, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar pruebas de acceso a la web para determinar el tipo de error que se está presentando.
		- Realizar aviso al proveedor de servicio web para solicitar soporte técnico.
* **Falla en la publicación de la página web de la ONS.**
	+ Dado el caso de la interrupción o falla en la página web de la Oficina Nacional de Semillas, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema que se está presentando.
		- Realizar aviso al proveedor de la página web para solicitar soporte técnico.
* **Fallo por bloqueos de seguridad en el servidor.**
	+ Dado el caso de la interrupción o falla en el acceso al servidor web la central telefónica por configuración, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema que se está presentando.
		- Realizar aviso al proveedor de la central para solicitar soporte técnico.

**Recursos de Contingencia**

Actualmente la Oficina Nacional de Semillas, cuenta con un contrato de manteniendo y soporte por parte de la empresa Arx de costa Rica Ltda., en donde brindan un soporte a la página web de la institución.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

## INDISPONIBILIDAD DE SISTEMA DE REGISTROS (USUARIOS, IMPORTACIONES, EXPORTACIONES).

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Fallo en acceso al sistema. | Usuarios del SistemasyClientes Externos. |
| Fallo en la funcionalidad del sistema. |
| Fallo en componentes del sistema por actualizaciones. |
| Fallo en la tablas de base de datos (Corruptas .dbf) |

**Tiempo aceptable de Caída**

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Fallo en acceso al sistema. | ALTO | 8 |
| 2. Fallo en la funcionalidad del sistema. | ALTO | 16 |
| 3. Fallo en componentes del sistema por actualizaciones. | ALTO | 16 |
| 4. Fallo en la tablas de base de datos (Corruptas .dbf) | ALTO | 24 |

**Causas de falla en el Sistema de Registros de Importaciones y Exportaciones.**

* **Fallo en acceso al sistema.**
	+ Dado el caso de fallo de acceso al sistema de registro de Importaciones y Exportaciones (Kronos), se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo del servidor de archivos compartidos en donde se encuentra el archivo de wsemilla.exe para determinar si se tiene acceso a la aplicación.
		- Realizar pruebas de acceso con otros usuarios para determinar si el problema de acceso es de una terminal o del usuarios, o bien si el problema se presenta a nivel institucional.
		- Realizar revisión de la plataforma de antivirus (Panda Adaptive Defense 360) para verificar que no sea un bloqueo de la aplicación en el antivirus.
		- Realizar aviso al proveedor de la aplicación para solicitar soporte técnico.
* **Fallo en la funcionalidad del sistema.**
	+ Dado el caso que se presenten fallas en la funcionalidad del sistema, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema con los usuarios expertos.
		- Realizar aviso al proveedor del sistema para solicitar soporte técnico.
* **Fallo en componentes del sistema por actualizaciones.**
	+ Dado el caso de la interrupción o fallo en el sistema por actualización de componentes requeridos por el aplicativo, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema que se está presentando.
		- Realizar pruebas de funcionalidad con otros usuarios para determinar si el problema se presenta solo en una terminal o bien si el problema se presenta a nivel institucional.
		- Validar los componentes externos que utiliza el sistema para determinar si requiere una actualización o un retorno al componente anterior.
		- Realizar aviso al proveedor del sistema para solicitar soporte técnico.

**Recursos de Contingencia**

Actualmente la Oficina Nacional de Semillas, cuenta con un contrato de manteniendo y soporte por parte de la empresa Kronosbi S.A., en donde brindan un soporte al sistema de registros de la institución.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

##

## INDISPONIBILIDAD DE SISTEMA DE REGISTROS VARIEDADES COMERCIALES.

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Fallo en acceso al sistema. | Usuarios del SistemasyClientes Externos. |
| Fallo en la funcionalidad del sistema. |
| Fallo en componentes del sistema por actualizaciones. |
| Fallo en la tablas de base de datos (Corruptas .dbf) |

Tiempo aceptable de Caída

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Fallo en acceso al sistema. | BAJO | 8 |
| 2. Fallo en la funcionalidad del sistema. | ALTO | 16 |
| 3. Fallo en componentes del sistema por actualizaciones. | ALTO | 16 |
| 4. Fallo en la tablas de base de datos (Corruptas .dbf) | ALTO | 24 |

**Causas de falla en el sistema de Registro de Variedades Comerciales.**

* **Fallo en acceso al sistema.**
	+ Dado el caso de fallo de acceso al sistema de registro de variedades comerciales (Kronos), se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo del servidor de archivos compartidos en donde se encuentra el archivo de kvari.exe para determinar si se tiene acceso a la aplicación.
		- Realizar pruebas de acceso con otros usuarios para determinar si el problema de acceso es de una terminal o del usuarios, o bien si el problema se presenta a nivel institucional.
		- Realizar revisión de la plataforma de antivirus (Panda Adaptive Defense 360) para verificar que no sea un bloqueo de la aplicación en el antivirus.
		- Realizar aviso al proveedor de la aplicación para solicitar soporte técnico.
* **Fallo en la funcionalidad del sistema.**
	+ Dado el caso que se presenten fallas en la funcionalidad del sistema, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema con los usuarios expertos.
		- Realizar aviso al proveedor del sistema para solicitar soporte técnico.
* **Fallo en componentes del sistema por actualizaciones.**
	+ Dado el caso de la interrupción o fallo en el sistema por actualización de componentes requeridos por el aplicativo, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema que se está presentando.
		- Realizar pruebas de funcionalidad con otros usuarios para determinar si el problema se presenta solo en una terminal o bien si el problema se presenta a nivel institucional.
		- Validar los componentes externos que utiliza el sistema para determinar si requiere una actualización o un retorno al componente anterior.
		- Realizar aviso al proveedor del sistema para solicitar soporte técnico.

**Recursos de Contingencia**

Actualmente la Oficina Nacional de Semillas, cuenta con un contrato de manteniendo y soporte por parte de la empresa Kronosbi S.A., en donde brindan un soporte al sistema de registros de la institución.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

## INDISPONIBILIDAD DE SISTEMA DE SEGUIMIENTO DE ACTIVIDADES DE CERTIFICACION Y CONTROL DE CALIDAD DE SEMILLAS (SACCS).

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Fallo en acceso al sistema. | Usuarios del SistemasyClientes Externos. |
| Fallo en acceso a la base de datos del sistema. |
| Fallo en la funcionalidad del sistema. |
| Fallo en componentes del sistema por actualizaciones. |

Tiempo aceptable de Caída

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Fallo en acceso al sistema. | BAJO | 8 |
| 2. Fallo en acceso a la base de datos del sistema. | ALTO | 16 |
| 3. Fallo en la funcionalidad del sistema. | ALTO | 16 |
| 4. Fallo en componentes del sistema por actualizaciones. | ALTO | 16 |

Causas de falla en el sistema de Seguimiento Actividades de Certificación y Control de Calidad de Semillas.

* **Fallo en acceso al sistema.**
	+ Dado el caso de fallo de acceso al sistema de SACCS, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato, encargado de mantenimiento del sistema.
		- Realizar pruebas de acceso con otros usuarios para determinar si el problema de acceso es de una terminal o del usuarios, o bien si el problema se presenta a nivel institucional.
		- Realizar revisión de la plataforma de antivirus (Panda Adaptive Defense 360) para verificar que no sea un bloqueo de la aplicación en el antivirus.
* **Fallo en acceso a la base de datos del sistema**
	+ Dado el caso de fallo de acceso al sistema de SACCS por fallo de comunicación con la base de datos, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato y encargado de mantenimiento del sistema.
		- Realizar un chequeo del archivo de configuración del sistema SACCS.EXE.Config para determinar que la conexión del sistema este direccionado al Servidor de base de datos correcto.
		- Realizar la revisión del Servidor virtual de base de datos que se pueda acceder, para determinar que el servidor está activo y en línea.
		- Realizar pruebas de acceso con otros usuarios para determinar si el problema de acceso es de una terminal o del usuarios, o bien si el problema se presenta a nivel institucional.
		- Realizar revisión de la plataforma de antivirus (Panda Adaptive Defense 360) para verificar que no sea un bloqueo de la aplicación en el antivirus.
* **Fallo en la funcionalidad del sistema.**
	+ Dado el caso que se presenten fallas en la funcionalidad del sistema, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar la solicitud de soporte al encargado de mantenimiento del sistema para que se haga la revisión del problema para su solución.
* **Fallo en componentes del sistema por actualizaciones.**
	+ Dado el caso de la interrupción o fallo en el sistema por actualización de componentes requeridos por el aplicativo, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema que se está presentando.
		- Realizar pruebas de funcionalidad con otros usuarios para determinar si el problema se presenta solo en una terminal o bien si el problema se presenta a nivel institucional.
		- Validar los componentes externos que utiliza el sistema para determinar si requiere una actualización o un retorno al componente anterior o bien buscar un nuevo componente que cumpla con las necesidades de la funcionalidad para solucionar el problema.

**Recursos de Contingencia**

Actualmente la Oficina Nacional de Semillas, cuenta el recurso humano encargado del soporte y mantenimiento del sistema de la institución.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

## INDISPONIBILIDAD DE SISTEMA DE ADMINISTRATIVO CONTABLE (ERP\_CONSULTANTS).

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Fallo en acceso al sistema. | Usuarios del Sistemas,Clientes y Proveedores. |
| Fallo en acceso a la base de datos del sistema. |
| Fallo en la funcionalidad del sistema. |
| Fallo en componentes del sistema por actualizaciones. |

Tiempo aceptable de Caída

|  |  |
| --- | --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |  |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO EN HORAS** |
| 1. Fallo en acceso al sistema. | BAJO | 8 |
| 2. Fallo en acceso a la base de datos del sistema. | ALTO | 16 |
| 3. Fallo en la funcionalidad del sistema. | ALTO | 16 |
| 4. Fallo en componentes del sistema por actualizaciones. | ALTO | 16 |

**Causas de falla en el sistema Administrativo Contable (ERP\_Consultants).**

* Fallo en acceso al sistema.
	+ Dado el caso de fallo de acceso al sistema de ERP\_Consultants, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato, encargado de mantenimiento del sistema.
		- Realizar pruebas de acceso con otros usuarios para determinar si el problema de acceso es de una terminal o del usuarios, o bien si el problema se presenta a nivel institucional.
		- Realizar revisión de la plataforma de antivirus (Panda Adaptive Defense 360) para verificar que no sea un bloqueo de la aplicación en el antivirus.
* **Fallo en acceso a la base de datos del sistema**
	+ Dado el caso de fallo de acceso al sistema de ERP\_Consultants por fallo de comunicación con la base de datos, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato y encargado de mantenimiento del sistema.
		- Realizar un chequeo del archivo de configuración del sistema, para determinar que la conexión del sistema este direccionado al Servidor de base de datos correcto y la Base de Datos SAAE.
		- Realizar la revisión del Servidor virtual que se pueda acceder, para determinar que el servidor está activo y en línea.
		- Realizar pruebas de acceso con otros usuarios para determinar si el problema de acceso es de una terminal o del usuarios, o bien si el problema se presenta a nivel institucional.
		- Realizar revisión de la plataforma de antivirus (Panda Adaptive Defense 360) para verificar que no sea un bloqueo de la aplicación en el antivirus.
* **Fallo en la funcionalidad del sistema**.
	+ Dado el caso que se presenten fallas en la funcionalidad del sistema, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar la solicitud de soporte al encargado de mantenimiento del sistema para que se haga la revisión del problema para su solución.
* **Fallo en componentes del sistema por actualizaciones.**
	+ Dado el caso de la interrupción o fallo en el sistema por actualización de componentes requeridos por el aplicativo, se debe tomar las acciones siguientes:
		- Realizar aviso al supervisor inmediato.
		- Realizar un chequeo previo al problema que se está presentando.
		- Realizar pruebas de funcionalidad con otros usuarios para determinar si el problema se presenta solo en una terminal o bien si el problema se presenta a nivel institucional.
		- Validar los componentes externos que utiliza el sistema para determinar si requiere una actualización o un retorno al componente anterior o bien buscar un nuevo componente que cumpla con las necesidades de la funcionalidad para solucionar el problema.

**Recursos de Contingencia**

Actualmente la Oficina Nacional de Semillas, cuenta el recurso humano encargado del soporte y mantenimiento del sistema de la institución.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

## INDISPONIBILIDAD DEL CENTRO DE CÓMPUTO

Impacto

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Fallo en la instalación Eléctrica del Centro de Computo Principal. | Todas las Áreas |
| Daño en el Servidor Principal por falla en hardware |
| Daño en el Servidor Principal por falla en software |
| Caída de la Red LAN: Servidores Windows y equipos de comunicación. |
| Daño en el Sistema de Enfriamiento del Centro de Computo Principal |
| Caída de la Red LAN: Servidores Windows y equipos de comunicación. |
| Interrupción de las comunicaciones Internas y Externas. |
| Paro de los sistemas que soportan las funciones de la Institución. |

**IDENTIFICAR IMPACTO DE LA CAIDA Y TIEMPOS ACEPTABLES DE CAIDA.**

|  |
| --- |
| **TIEMPOS ACEPTABLES DE CAIDA.** |
| **RECURSO** | **PRIORIDAD DE RECUPERACION** | **TIEMPO HORAS** |
| 1. Servidor físico Principal (No se tendrá Acceso a ninguna plataforma de la ONS). | ALTO | 24 |
| 2. Servidor de Dominio. (No se contara con acceso a los equipos de la ONS). | ALTO | 24 |
| 3. Servidor Base de Datos (No se contara con acceso a los sistemas de la ONS). | ALTO | 24 |
| 4. Servidor Archivos (No se contara con acceso a los archivos y documentos de funcionarios de la ONS). | ALTO | 24 |
| 5. Centro de Telecomunicaciones (Red Interna de la ONS) | ALTO | 24 |
| 6. Servidor de Firewall (No se contara con una seguridad de tráfico de la web). | MEDIA | 24 |
| 7. Central Telefónica IPS (No se tendrá acceso a las llamadas telefónicas de la Oficina Entrantes y Salientes).  | MEDIA | 24 |

**Recursos de Contingencia**

* Si es necesario, el hardware y software necesarios que se deben tener o adquirir, como parte de las estrategias básicas para disponer de equipo de reemplazo son:
	+ Acuerdos con proveedores: Se establecen acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.
	+ Inventario de equipos: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura.
	+ Equipo Compatible Existente: Equipo existente en sitios alternativos.
* Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación.
* Almacenar un equipo sin usar es costoso, pero permite que la recuperación comience más rápidamente.
* Considerar la posibilidad de un desastre extendido que requiere reemplazos masivos de equipos y retrasos del transporte.
* Mantener listas detalladas de necesidades de equipo y especificaciones dentro del plan de contingencia.

**Recursos de Contingencia Generales**

* Router
* Servidores y Equipos de Comunicación (Switchs, Fibra, etc.).
* Gabinete de Comunicaciones y Servidores.
* Materiales y herramientas para cableado estructurado.
* UPS y Equipos de aire acondicionado.
* Backup de los Sistemas.
* Instaladores de las aplicaciones, de Software Base, Sistema Operativo, Utilitarios, etc.

## AUSENCIA PARCIAL O PERMANTE DEL PERSONAL DE TI.

**Impacto**

|  |  |
| --- | --- |
| **IMPACTO** | **ÁREA AFECTADA** |
| Interrupción de funciones de la persona ausente | Todas las Áreas |
| – Administración de bases de datos.– Control y monitoreo de servidores.– Soporte a los usuarios.– Ajustes a programas críticos en producción |

**Recursos de Contingencia**

Actualmente se cuenta con dos funcionarios que en caso de faltar uno el otro debe suplir en las funciones de continuidad del negocio, para su puesta en marcha lo más antes posible.

Nota: Ver Anexo 1 para encontrar el contacto del proveedor del servicio.

PLAN DE VERIFICACION Y PRUEBAS

Tres medidas de minimizar los riesgos de la tecnología son la:

* Verificación
* Prueba
* Mantenimiento de los sistemas.

Cada componente de un sistema de cómputo equipo, comunicaciones y programas debe ser verificado y probado rigurosamente antes de utilizarlo para un evento.

PLAN DE VERIFICACIÓN

Para el Plan de Contingencia es muy importante y es conveniente que se pueda realizar la verificar que una autoridad independiente aplique las pruebas de verificación.

Para sistemas de menor importancia, la verificación puede realizarse internamente.

Las pruebas de verificación (también conocidas como pruebas de calidad) pueden incluir:

• Probar los equipos bajo condiciones que simulen las de operación real.

• Probar los programas para asegurar que se siguen los estándares apropiados y que desempeñan las funciones esperadas.

• Asegurar que la documentación sea la adecuada y esté completa.

• Asegurar que los sistemas de comunicación se adecue a los estándares establecidos y funcionen de manera efectiva.

• Verificar que los sistemas sean capaces de operar bajo condiciones normales, pero también bajo potenciales condiciones inesperadas.

• Asegurar que se cuente con las debidas medidas de seguridad y que estas se adecuen a las normas establecidas.

## PROCEDIMIENTO PARA LAS PRUEBAS DEL PLAN DE CONTINGENCIA

Todos los planes de contingencia deben ser probados para demostrar su habilidad de mantener la continuidad de los procesos críticos de la Oficina Nacional de Semillas.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos.

### OBJETIVO

El objetivo principal, es determinar si el Plan de contingencia es capaz de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos de la Oficina Nacional de Semillas, probando la efectividad de los procedimientos expuestos en el plan de contingencias.

Las pruebas permiten efectuar una valoración detallada de los costos de operación en el momento de ocurrencia de una contingencia.

### MÉTODOS DE PRUEBAS DE CONTINGENCIA

1. **Prueba Específica**

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencia. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

1. **Prueba de Escritorio**

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas.

**Características:**

* La discusión se basa en un formato preestablecido.
* Está dirigido al equipo de recuperación de contingencias.
* Permite probar las habilidades gerenciales del personal que tiene una mayor responsabilidad.

Los ejercicios de escritorio son ejecutados por el encargado de la prueba y el personal responsable de poner el plan de contingencias en ejecución, en una situación hipotética de contingencia. Un conjunto de preguntas se pedirán que resuelva el personal. El encargado y el personal utilizarán el plan de contingencias para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos

 necesarios están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

1. **Simulación en Tiempo Real**

Las pruebas de simulación real, en una Unidad Orgánica, a nivel de Gerencia en la Oficina Nacional de Semillas, está dirigido a una situación de contingencia por un período de tiempo definido.

* Las pruebas se hacen en tiempo real.
* Son usadas para probar partes específicas del plan.
* Permiten probar las habilidades coordinativas y de trabajo en equipo de los grupos asignados para afrontar contingencias.

**Preparaciones PRE Prueba**

* Repasar el plan de contingencia.
* Verificar si se han asignado las respectivas responsabilidades.
* Verificar que el plan este aprobado por la alta dirección de la institución.
* Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
* Establecer la fecha y hora para la ejecución de la prueba.
* Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.
* Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.
* No dejar de lado los resultados obtenidos, la meta es aprender y descubrir las vulnerabilidades, no generar fracaso y frustración.
* La prueba inicial se enfoca principalmente en entrenar al equipo que ejecutará con éxito el plan de contingencias, solucionando el problema y restableciendo a la normalidad las actividades realizadas.
* Enfocar los procesos críticos que dependen de la Oficina Nacional de Semillas
* Definir el ambiente donde se realizarán las reuniones del equipo de recuperación de contingencias.
* Distribuir una copia de la parte del Plan de Contingencias a ser ejecutado.

**Comprobación de Plan de Contingencias**

La prueba final debe ser una prueba integral que involucre todas las áreas de trabajo de la oficina Nacional de Semillas. La capacidad funcional del plan de contingencia radica en el hecho de que tan cerca se encuentren los resultados de las pruebas con las metas planteadas.

# ANEXOS

# LISTADO DE PROVEEDORES DE SERVICIOS Y CONTACTOS.

A continuación se presenta el cuadro con contactos de proveedores de servicios.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **EMPRESA** | **SERVICIO** | **CONTACTO** | **TELEFONO** | **CELULAR** | **CORREO** | **PAGINA WEB** |
| I.C.E. | Telefonía e Internet | Servicio al Cliente | 1119 |   |   | <https://www.kolbi.cr/> |
| TIGO CR | Internet | Servicio al Cliente | 800-007-9637 |   |   | <https://www.tigo.cr/> |
| COCOCO CR | Hardware y Software | Adrian Sancho | 2202-8923 | 8399-3404 | adrian.sancho@grupo3c.com | <https://www.cococo.co.cr/> |
| CDC Internacional | Hardware y Software | Denia Madrigal | 2258-3444 | 8879-7856 | dmadrigal@cdcinternacional.com | <https://www.cdcinternacional.com/> |
| Intelect Costa Rica | Hardware y Software | Tatiana Tenorio | 2202-1311 |   |   | [www.intelec.co.cr](http://www.intelec.co.cr/) |
| Componentes el Orbe | Hardware y Software | Servicio al Cliente | 2545 47-00 |   |   | <http://elorbe.la/home-public/> |
| KRONOS SISTEMAS, S.A.  | Proveedor de Sistemas | Manuel Vargas | 2229-0998 | 8813-7969 |   |   |
| TRIGONA HOSTING | Proveedor de Hosting | Max Bogarin | 2214-9097 | 8863-6035 |   | <http://www.trigonahosting.com/> |
| Arx de costa Rica Ltda. | Página Web O.N.S. | Lidia Noches |   | 8894-6414 | lidia.noches@gmail.com |   |