PERÚ | Ministerio de Desarrollo Agrario y Riego

SERFOR
Firmado digitalmente por MANCO SUNI Enrique Julio FAU 20562836927 soft
Motivo: Soy el autor del documento
Fecha: 02.06.2021 14:21:42 -05:00

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL SERVICIO NACIONAL FORESTAL Y DE FAUNA SILVESTRE

Formulada por : Oficina de Tecnologías de la Información.

SERFOR
Firmado digitalmente por RENGIFO CASTILLO Ivan David FAU 20562836927 soft
Motivo: Soy el autor del documento
Fecha: 02.06.2021 12:15:10 -05:00

SERFOR
Firmado digitalmente por OLIVA ORTIZ Javier Emilio FAU 20562836927 soft
Motivo: Soy el autor del documento
Fecha: 02.06.2021 12:21:13 -05:00

SERFOR
Firmado digitalmente por AMAYA CASTILLO Jorge Augusto FAU 20562836927 soft
Motivo: Soy el autor del documento
Fecha: 16.06.2021 21:17:25 -05:00

SERFOR
Firmado digitalmente por LOBATON COTITO Martin Felix FAU 20562836927 soft
Motivo: Soy el autor del documento
Fecha: 02.06.2021 12:32:51 -05:00

Firmado digitalmente por VALENCIA HUANCA Yury Edwin FAU 20562836927 soft
Motivo: Soy el autor del documento
Fecha: 02.06.2021 13:01:07 -05:00

ÍNDICE

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL SERVICIO NACIONAL FORESTAL Y DE FAUNA SILVESTRE

I. INTRODUCCIÓN

Las tecnologías de la información y la automatización de los procesos son elementales en el éxito de toda institución gubernamental o privada, considerando que los servicios que estos proveen son críticos y necesarios para el logro de sus objetivos; motivo por el cual se debe garantizar su completa operatividad minimizando la presencia de interrupciones.

El presente Plan de Contingencia, muestra las pautas y procedimientos que deberán ser ejecutadas en cada uno de los eventos que alteren el normal funcionamiento de los servicios críticos. Del mismo modo, se detallan alcances conceptuales que permitirán a la persona que accede a este documento reforzar y ampliar sus capacidades para que pueda familiarizarse con el plan de contingencia y la capacidad de reaccionar ante eventos inesperados que pueda ocasionar la paralización de las actividades en el ámbito de las TIC; también puede considerarse como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencias.

La elaboración del Plan de Contingencia de TI implica un importante avance a la hora de superar situaciones de interrupción en las actividades y servicios prestados por la OTI, siendo indispensable para el éxito del mencionado Plan, poder contar con el personal involucrado, capacitado y comprometido con la continuidad de las operaciones en la entidad.

II. OBJETIVO

Objetivo General

Garantizar la continuidad operativa de los servicios críticos de Tecnologías de Información que brinda el SERFOR, ante la presencia de incidentes que puedan alterar su normal funcionamiento, restableciéndolo en el menor tiempo posible, a través de la puesta en marcha del plan que contempla los procedimientos, actividades y elementos requeridos para afrontar la contingencia.

Objetivos específicos

- Prevenir o minimizar los daños o pérdida de archivos digitales de Tecnologías de la Información.
- Minimizar las potenciales pérdidas económicas de la Institución
- Reducir los tiempos de interrupciones en los servicios críticos de información.
- Reducir las interrupciones en las operaciones críticas de las diferentes áreas de la Institución
- Prevenir o minimizar los daños a los recursos informáticos.

- Facilitar una recuperación ordenada de los archivos digitales y Sistemas informáticos críticos de la Institución.
- Proteger los activos informáticos de la institución.
- Ampliar la seguridad física del personal y de los clientes
- Minimizar la necesidad de toma de decisiones durante un incidente.

III. ALCANCE

El presente Plan de Contingencia de Tecnologías de la Información es de aplicación en todas las dependencias de SERFOR a nivel Nacional, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por la Oficina de Tecnologías de la Información del SERFOR, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

IV. DOCUMENTOS DE REFERENCIA

4.1. Norma Técnica Peruana NTP ISO/IEC 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

4.2. Resolución Ministerial N° 028-2015-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de las Entidades Públicas en los tres niveles de Gobierno.

4.3. Decreto Supremo N° 111-2012-PCM, que incorpora la Política Nacional de Gestión de Riesgos de Desastres de cumplimiento obligatorio para las entidades del Gobierno Nacional.

4.4. “Guía práctica para el desarrollo de Planes de Contingencia de Sistemas de Información” – Elaborado por INEI el 2001.

V. DEFINICIONES

5.1. Activo de información: Comprende a cada elemento que soporta la información, es decir que la contiene, la procesa y la transporta.

5.2. Amenaza: Causa potencial de un incidente no deseado.

5.3. Contingencia: Se define como contingencia a la alteración en la continuidad del negocio, que impacta en forma relevante el normal desarrollo de un servicio considerado crítico,

teniendo su origen en la falla de uno o varios componentes o la interrupción de una tarea, sin estar necesariamente prevista.

5.4. Impacto: Resultado de un suceso o evento de contingencia.

5.5. Punto de Recuperación Objetivo (RPO): El objetivo del punto de recuperación (RPO) se utiliza como métrica para la recuperación de los datos. También se mide en términos de tiempo, pero hace referencia a la edad o a la frescura de los datos requeridos para restaurar la operación que sigue a un acontecimiento adverso. Los datos, en este contexto, pueden también incluir la información con respecto a las transacciones no registradas o no capturadas. Como el RTO, cuanto más pequeño es el RPO, más alto son los costos de la recuperación prevista de los datos.

5.6. Plan de contingencia: Es el proceso para desarrollar, comunicar y mantener documentados y aprobadas las acciones que permitan restituir rápidamente los servicios tecnológicos de la organización ante una eventualidad que pueda paralizar, ya sea de forma parcial o total de la Institución.

5.7. Probabilidad: Posibilidad de que algún evento de contingencia se materialice.

5.8. Riesgo: Incertidumbre que podría desencadenar una interrupción indeterminada en los servicios de TI.

5.9. Riesgo Operativo: Riesgo vinculado a la administración y supervisión del personal.

5.10. Riesgo Técnico: Riesgo vinculado a fallas en los suministros de energía y servicios complementarios.

5.11. Riesgo Tecnológico: Riesgo vinculado a los servicios de tecnologías de la información.

5.12. Servicio crítico: Servicio de gran valor para el cumplimiento de los objetivos del SERFOR.

5.13. Tiempo de inactividad o downtime: El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible. Los casos de dowtime pueden ser Planeado o No planeados.

Downtime no Planeado	Falla del Sistema
	Fallas de Data
Downtime Planeado	Cambio del Sistema
	Cambios de Data

5.14. El Tiempo de Recuperación Objetivo (RTO) es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. Debe medirse desde el momento en que ocurre la interrupción hasta que se reanude la operación.

5.15. Tiempo de recuperación de componentes: Es el tiempo requerido por cada actividad involucrada en la restauración de un servicio. Una falla en cualquiera de los componentes de las actividades podría conducir a un incumplimiento del RTO. Con este fin, a cada componente de la actividad se puede asignar un RTO. La sumatoria de cada uno de los RTOs de estos componentes no necesariamente equivale al RTO del servicio, porque las actividades pueden ser llevadas a cabo en paralelo.

5.16. Tiempo de recuperación de la red: Es el tiempo para restaurar la comunicación de datos y voz después de un evento adverso. Esta posiblemente tendrá impacto sobre otras actividades.

5.17. Tiempo de recuperación de datos: Es el tiempo para extraer los datos de respaldo del soporte de almacenamiento y enviarlos al sitio de recuperación, sea físicamente (mediante trasporte) o electrónicamente (vía red). Incluye el tiempo de cargar los datos desde el medio (cinta, disco), instalar o reiniciar la aplicación de base de datos.

5.18. Tiempo de recuperación de aplicaciones: Es el tiempo para corregir una aplicación en mal funcionamiento.

5.19. Tiempo de recuperación de plataforma: Es el tiempo para restaurar una plataforma problemática para la operación de servicios.

5.20. Tiempo de recuperación del servicio: Representa el tiempo acumulado para restaurar el servicio desde la perspectiva del usuario final.

5.21. UPS: Dispositivo alterno de almacenamiento de energía eléctrica.

5.22. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5.23. Ataque de Día Cero: Un ataque de día cero es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de

vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto.

5.24. MTD: Se define como el Tiempo de inactividad máximo tolerable que define la cantidad total de tiempo que un proceso de negocio puede interrumpirse sin causar consecuencias inaceptables.

VI. DIAGNÓSTICO Y SITUACION ACTUAL DE LAS TECNOLOGIAS DE LA INFORMACION

6.1. Infraestructura Tecnológica y recursos informáticos existentes.

SERFOR posee una configuración de red jerarquizada, conformada por dos switches de marca CISCO modelo 2960, con el rol o función de core, con conexiones de 10 Gbps de velocidad. Asimismo, existen switches de la misma marca de enlace y distribución, sin embargo las conexiones backbone y las conexiones a los servidores poseen velocidades de 1 Gbps, lo cual puede representar cuellos de botella.

Para la protección perimetral, SERFOR posee un Firewall UTM (appliance) de marca SOPHOS y un segundo firewall como contingencia de marca CISCO modelo ASA 5508x (para activar la contingencia se requiere una configuración manual), definiendo configuraciones de red LAN, DMZ y WAN, como se apreciar en la figura.

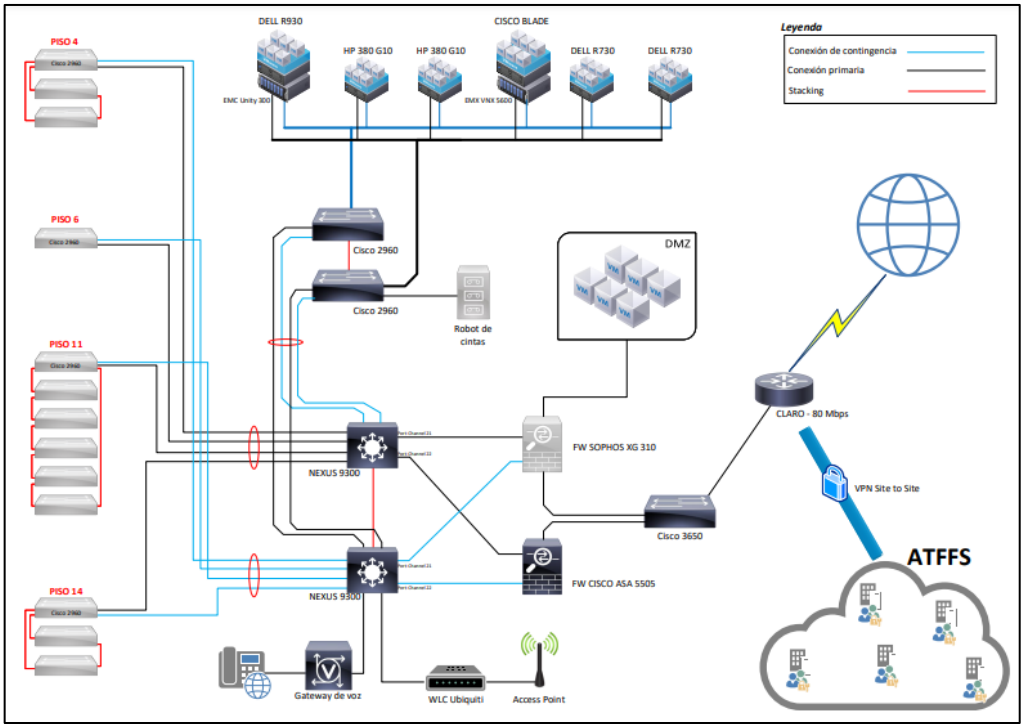


Figura N° 1: Diagrama Lógico de Red de SERFOR (Fuente: Proporcionada por el área de Infraestructura Tecnológica de OTI)

Existen aplicaciones publicadas en internet, que no están ubicadas en la zona desmilitarizada (DMZ) y bases de datos en la zona DMZ, ambas configuraciones representan vulnerabilidades ante ataques desde internet, por lo que se ha considerado realizar un ordenamiento de aplicaciones y bases de datos para el periodo 2021.

La plataforma de procesamiento se basa en 07 servidores virtualizados, así como unidades de almacenamiento interconectadas directamente a servidores en una red de datos LAN, considerar un total de 1.2 TB de memoria RAM y 80 TB de almacenamiento. En la siguiente tabla se puede apreciar los servidores virtualizados y el consumo de CPU, memoria RAM y consumo de almacenamiento en disco.

Equipo servidor	Consumo CPU	Consumo RAM	Consumo almacenamiento
Dell R930	13%	86%	86%
Dell 730	5%	31%	71%
Dell 730	15%	89%	83%
HP DL 380	23%	71%	81%
HP DL 380	13%	80%	63%
Cisco Blade UCS B200	46%	86%	74%
Cisco Blade UCS B200	2.7%	3%	59%

El servidor Dell R930 es el de mayor capacidad y soporta aproximadamente el 80% de las aplicaciones de SERFOR, el consumo de memoria RAM y almacenamiento de dicho equipo, exceden lo recomendable (no se recomienda exceder el consumo de 70% para memoria RAM y almacenamiento), considerando que, por el tipo de información, el almacenamiento seguirá creciendo y estando al límite de su capacidad, representa un riesgo alto. En general, existe un alto consumo de memoria RAM y almacenamiento en la mayoría de los servidores, representando un riesgo alto. Adicionalmente, se debe considerar que los dos servidores Dell 730, indicados en la tabla, son prestados, de propiedad del Programa Forestal.

La virtualización está basada en el sistema VMware ESXi versiones 5.5, 6.0 y 6.7 y un total de aproximadamente 120 servidores virtualizados (máquinas virtuales), los mismos que no se encuentran en una configuración de alta disponibilidad por falta recursos y de cluster de virtualización.

Al respecto, se tiene considerado adquirir para el periodo 2021, servidores en configuración cluster y unidades de almacenamiento, toda la configuración en alta disponibilidad.
Los sistemas operativos de los servidores son Windows Server 2003R2/2008/2008R2/2012R2/2016 y Linux Ubuntu/Centos.

Los órganos desconcentrados ATFFS tienen equipamiento en redes independiente y con conexiones de internet ADSL, que dificulta la administración de dicho equipamiento y genera vulnerabilidades en el acceso a internet de los usuarios de los órganos desconcentrados.

La sede Central cuenta con un enlace de internet de 80MB, el mismo que no tiene un enlace de contingencia.

Existe personal trabajando desde sus casas, en la modalidad de escritorio remoto, bajo tecnología VPN y el protocolo de encriptación IPsec, servicio que brindan eficientemente los firewalls. Sin embargo, no existe procedimientos para su uso, por lo que se tiene previsto elaborar lineamientos para trabajo remoto para el periodo 2021.

- Licencias Sistemas Operativos

Descripción	Estaciones de Trabajo
Microsoft Windows 10 Pro	291
Microsoft Windows 7 Professional	398
Microsoft Windows 7 Ultimate	2
Microsoft Windows 8 Pro	5
Microsoft Windows 10 Pro for Workstations	2
Total	698

- Lenguaje de Programación

Descripción	Pc Instalados
Java	5
PowerBuilder	1
Visual Basic .Net	1
C#	4
Visual Fox	1
PHP	2
Total	17

- Entorno de Desarrollo Integrado (IDE)

Descripción	PC Instalados
ECLIPSE	3
Visual code	3
Visual Estudio .NET	4
Total	10

- Servidor de Aplicaciones Web

Descripción	Cantidad
Internet Information Services	5
Apache web	2
Apache tomcat	5
Glassfish	4
Total	16

- Licencias ArcGis

Descripción	Operativos
ArcGIS Enterprise Advanced for Windows up to four cores	1
ArcGIS Desktop Advanced CU	10
ArcGIS 3D Analyst for Desktop CU	10
ArcGIS Spatial Analyst for Desktop CU	10
Total	31

- Servidores

Descripción	Operativos
Servidor Dell R930	1
Servidor Dell R730	2
Servidor Dell R740	1
Servidor HP DL380 G10	2
Servidor Cisco Blade UCS B200	2
Total	8

- Gestor de Base de Datos

Descripción	Servidores Instalados
Microsoft SQL Server	5

- Correo electrónico corporativo
  Se cuenta con G suite con el servicio de correo Gmail.

Descripción	Cantidad licencias
Gmail	800

- Gestor de Contenidos

Descripción	Uso
WordPress	Si
Joomla	Si

- Servidores Virtualizados

Descripción	Cantidad
Windows Server 2016	4
Windows Server 2016	26
Windows Server 2012	25
Windows Server 2008	9
Windows Server 2003	1
Ubuntu Linux 64 bits	12
Debian GNU/Linux 7	2
Centos 7	4
Centos 6.1	1
Centos 6	1
Total	85

6.2. Sistemas de Información y Aplicativos

El inventario de las aplicaciones TI, servicios tecnológicos, software y hardware analizados se presentan a continuación clasificados según sus urgencias de recuperación.

Estas urgencias de recuperación han sido definidas en función del mínimo tiempos de recuperación definidos en cada evento desarrollado en capítulo de estrategia. Esta

información permitirá a la Oficina de Tecnología afinar la definición de sus estrategias de recuperación alineadas con las necesidades de la Institución.

N°	SISTEMA Y/O APLICACIÓN	DESCRIPCIÓN	AREA PROPIETARIA
1	SGD	Sistema de Gestión Documental	Oficina de Servicios al Usuario y Trámite Documentario
2	AlertaSerfor	Sistema de Denuncias Forestales y de Fauna Silvestre	Dirección de Control de la Gestión del Patrimonio Forestal y de Fauna Silvestre
3	Bambu	Reporte del registro de plantaciones de bambú	Dirección de Gestión Sostenible del Patrimonio Forestal
4	Incendioforestal	Sistema de ocurrencia de incendios forestales	Dirección de Gestión Sostenible del Patrimonio Forestal
5	Infractores	Sistema Registro Nacional de Infractores	Dirección de Información y Registro
6	Leyconcordada	Sistema de Ley Forestal y de Fauna Silvestre Concordada (Consulta)	Dirección de Política y Regulación
7	Leyconcordadagestion	Sistema de Ley Forestal y de Fauna Silvestre Concordada (Administración)	Dirección de Política y Regulación
8	Libro de operaciones de centros de transformación primaria	Libro de operaciones de centros de transformación primaria	Dirección de Control de la Gestión del Patrimonio Forestal y Fauna Silvestre
9	Portal Web	Portal web de la institución, se elaboró en sistema de gestión de contenidos (CMS) wordPress.	Oficina de Comunicaciones
10	RecursosTI	Sistema de Gestión de Accesos a Recursos Informáticos, requerimientos de bienes y servicios de tecnologías de información y Mesa de Ayuda	Oficina de Abastecimiento
11	RNPF	Sistema del Registro Nacional de Plantaciones Forestales	Dirección de Información y Registro
12	Sniffs	Sistema de inspección de guía de transporte forestal	Dirección de Control de la Gestión del Patrimonio Forestal y Fauna Silvestre
13	Siscites	Sistema de emisión y control de permisos y certificados CITES	Dirección de Gestión Sostenible del Patrimonio Forestal

N°	SISTEMA Y/O APLICACIÓN	DESCRIPCIÓN	AREA PROPIETARIA
14	Sisrehu	Sistema de la Oficina de Recursos Humanos - Gestión de Personal y Asistencia	Oficina de Recursos Humanos
15	SIGAWEB	Sistema Integrado de Gestión Administrativa - SIGA	Oficina de Abastecimiento
16	Sistema de Mesa de Partes Virtual	Sistema de Mesa de Partes Virtual	Oficina de Servicios al Usuario y Trámite Documentario
17	Sisged	Sistema de Gestión Documentaria	Oficina de Servicios al Usuario y Trámite Documentario
18	Servicio de orientación vía web	Servicio de orientación vía web mediante el cual se proporciona información sobre los servicios y trámites que se realizan en la entidad.	Oficina de Servicios al Usuario y Trámite Documentario
19	SerforRRHH	Sistema Empresarial de Recursos Humanos	Oficina de Recursos Humanos
20	Sifweb	Sistema de intranet INRENA	No identificada
21	TransparenciaV03	Sistema de transparencia	Oficina de Servicios al Usuario y Trámite Documentario
22	VVMantto	Sistema de Mantenimiento y Configuración de Ventanilla Virtual	Oficina de Servicios al Usuario y Trámite Documentario
23	WebRRHH	Sistema web de recursos humanos	Oficina de Recursos Humanos
24	LibroReclamaciones	Sistema libro de reclamaciones	Oficina de Servicios al Usuario y Trámite Documentario
25	Mcsmaestra	Servicio de consultas	Dirección de Control de la Gestión del Patrimonio Forestal y Fauna Silvestre
26	SIAF	Sistema de Presupuesto	Oficina de Planeamiento y Racionalización
27	CEPLAN	Sistema de Presupuesto	Oficina de Planeamiento y Racionalización

6.3. Servicios Tecnológicos

N°	NOMBRE DEL SERVICIO	DESCRIPCIÓN	AREA PROPIETARIA
1	ACCESO A INTERNET	Servicio de internet del SERFOR	Oficina de Tecnología de la Información
2	CORREO ELECTRONICO	Servicio de mensajería electrónica del SERFOR	Oficina de Tecnología de la Información
3	DIRECTORIO ACTIVO	Servicio de administración de inicios de sesión en los equipos conectados a la red del SERFOR, así como también la administración de políticas en toda la red.	Oficina de Tecnología de la Información
4	PAGINA WEB	Servicio de administración de información y recursos de carácter público.	Oficina de Tecnología de la Información
5	INTRANET	Servicio de administración de información y recursos internos a la red del SERFOR.	Oficina de Tecnología de la Información
6	SOPORTE TECNICO	Servicio de soporte técnico del SERFOR	Oficina de Tecnología de la Información

6.4. Software y Respaldo de Información

N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	AREA PROPIETARIA
1	SOFTWARE	Para este activo se refiere: base de datos y desarrollo, antivirus, sistemas operativos, ofimática, software para monitoreo	Oficina de Tecnología de la Información
2	RESPALDO DE INFORMACIÓN	Activos de respaldo para: base de datos, sistemas de información, portal web y archivos, configuración.	Oficina de Tecnología de la Información

6.5. Hardware y Comunicaciones

N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN	Alta disponibilidad	Estado	Año	AREA PROPIETARIA
1	REDES Y COMUNICACIONES	Servidores físicos Switch Router Firewall UPS Cableado estructurado	SI	Sin Soporte (*)	2014	Oficina de Tecnología de la Información
2	SISTEMAS DE APOYO	Sistema de aire acondicionado	NO	Sin Soporte (*)	2022	Oficina de Tecnología de la Información
3	SISTEMAS DE APOYO	Sistema de energía eléctrica (UPS)	NO	Con Soporte	2020	Oficina de Tecnología de la Información

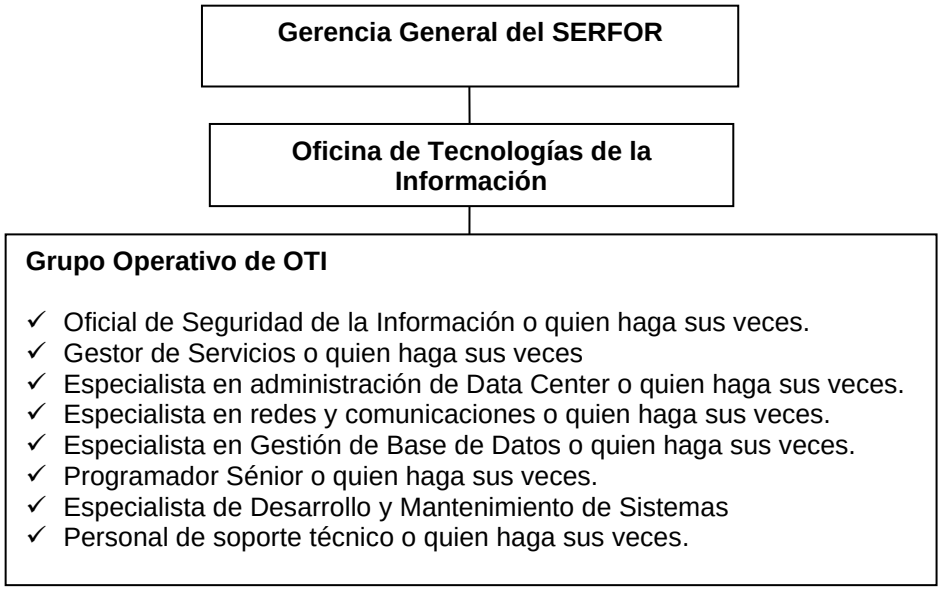
(*) Se considerado su renovación de soporte y mantenimiento en el prepuesto a partir del próximo año (2022).

6.6. Organización y equipo responsable

a. Uno de los aspectos que evidencia un carácter formal y serio en toda entidad es que se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria, mientras dure dicho evento.

b. Es necesario entonces que el Plan de Contingencia de TI deba hacerse de manera formal y responsable involucrando a toda la entidad y definiendo un grupo responsable para su elaboración, validación y mantenimiento.

Equipo de Contingencia de TI



6.7. Funciones y Responsabilidades

a. La Gerencia General
- Participar en las reuniones periódicas propuestas por el Director de la OTI.
- Proponer, aprobar o rechazar la incorporación y/o modificaciones del Plan de Contingencia TI
- Aprobar los informes presentados por el Director de OTI
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados.
- Realizar las coordinaciones para contar con la disponibilidad de recursos necesarios para soportar la operativa y la restauración de los servicios afectados por algún evento imprevisto.

b. La Dirección de la Oficina de Tecnologías de la Información es responsable de:
- Gestionar los recursos necesarios para el correcto desempeño del Plan de Contingencia de TI.
- Informar a la Dirección Ejecutiva sobre la materialización de algún evento de contingencia y sus resultados.
- Activar/Desactivar la ejecución del Plan de Contingencia de TI.
- Informar a las Unidades Orgánicas sobre la ocurrencia del evento de contingencias y coordinar las acciones necesarias.
- Supervisar la ejecución de las actividades del Plan Contingencia de TI.

c. El Oficial de Seguridad de la Información es responsable de:
- Elaborar, revisar, presentar y mantener actualizado el Plan de Contingencias de TI.
- Ejercer control y seguimiento del Plan de Contingencia de TI.

- Coordinar la ejecución del Plan de Contingencia de TI.
- Informar a la Jefatura de TI sobre los resultados obtenidos en el desarrollo del Plan de Contingencia de TI
- Coordinar simulacros periódicos en relación con el Plan de Pruebas con el fin de mantener activos a los miembros del equipo y la vigencia del Plan de Contingencia de TI.
- Verificar que el personal involucrado este permanentemente capacitado respecto a su función dentro del Plan de Contingencia de TI.

d. Gestor de Servicios de TI
   - Mantener permanentemente actualizado el Plan de Contingencia.
   - Coordinar la ejecución del Plan de Contingencia cuando se presenten los eventos que lo activan.
   - Evaluar el impacto de las contingencias que se presenten.
   - Elaborar los informes mensuales referidos al Plan de Contingencia.
   - Proponer, al Comité de Contingencia, la incorporación de nuevos eventos de riesgo en el Plan de Contingencia.
   - Capacitar al personal nuevo del servicio sobre las actividades que deben de ejecutar cuando se presenta la contingencia.
   - Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el Plan de Contingencia.
   - Proponer reuniones periódicas sobre el Plan de Contingencia.

e. Especialista en administración de Data Center
   - Verificar la activación automática de los equipos de energía.
   - Comunicar a todas las Unidades Orgánicas del SERFOR del evento.
   - Apagar los servicios los equipos de seguridad perimetral, comunicaciones y servidores que alojen los Sistemas.
   - Monitorear el uso de equipos de energía para el restablecimiento
   - Coordinar con las UO afectadas de tomar las medidas necesarias.

f. Especialista en redes y comunicaciones
   - Verificar la magnitud del fallo o avería en las redes de comunicación
   - Notificar al proveedor de Servicios de redes y comunicaciones.
   - Supervisar al proveedor para el restablecimiento de los servicios.
   - Monitorear que los servicios se encuentren en línea.

g. Especialista en Gestión de Base de Datos
   - Configurar las bases de datos de respaldo
   - Restaurar la copia de seguridad más reciente
   - Verificar la existencia del servidor nuevo en el dominio.
   - Informar a los usuarios la nueva ruta de la base de datos del aplicativo

h. Programador Sénior, especialista de Desarrollo y Mantenimiento de Sistemas
   - Revisar el sistema de Información o aplicativo dañado
   - Hacer pruebas al sistema de Información o aplicativo una vez solucionada la falla.
   - Verificar los permisos sobre el sistema de información o aplicativo.

- Informar a los usuarios la ruta del servidor del aplicativo.

i. Personal de soporte técnico
   - Verificación al equipo asignado para su diagnóstico y solución.
   - Preparar los equipos de cómputo para su remplazo.
   - Solicitar conformidad de la atención

VII. METODOLOGIA DESARROLLO DEL PLAN DE CONTINUIDAD TECNOLOGICA

La metodología de referencia utilizada es la BCM (Business Continuity Management), la cual nos permite definir y establecer el Plan de Contingencia para reducir el impacto provocado por una paralización total o parcial de la operación de la Institución y garantizar así, la recuperación ágil y progresiva de los servicios tecnológicos y procesos críticos afectados.

La continuidad operativa del SERFOR dependerá del evento y/o desastre sucedido y ante ello se debe asegurar los procesos y servicios tecnológicos críticos, según la estrategia desarrollada.

Para la elaboración del plan de contingencia tecnológico se han establecido las siguientes fases:

1. Planificación: Se definido y preparado los esfuerzos de planificación de las actividades en cada etapa de contingencia (Prevención, Ejecución y Recuperación).

2. Identificación de Riesgos: Se minimiza las fallas generadas por los eventos en contra del normal desempeño de los sistemas de información a partir del análisis de la criticidad de los eventos identificados.

3. Identificaciones de soluciones: Para reducir los costos se han establecido soluciones en la medida de lo posible, a tiempo de documentar los riesgos de fallas e interrupciones identificadas.

4. Estrategias: Se identifican las prioridades y se determina en forma razonable las actividades hacer implementadas en cada etapa desarrollada (Prevención, Ejecución y Recuperación)

5. Documentación del proceso: Desarrollo de procedimientos y/o actividades en las etapas de prevención, ejecución y recuperación desarrolladas en cada evento.

6. Realización de pruebas: Se identificado los escenarios/eventos con probabilidad de recuperación aceptable por la Institución a través de actividades en cada etapa de recuperación.

7. Monitoreo: Se han establecido las actividades preventivas y mantenimiento que permita reaccionar en el tiempo preciso y se tomen las acciones correctas.

Las consecuencias que puede ocasionar a la Institución la materialización de los riesgos, a continuación se detallan las actividades para determinar el nivel de impacto:

a. Niveles de Impacto de Negocio: Se identifican los servicios y sistemas de tecnología de información que son utilizados para apoyar la misión, visión, objetivos y metas de la institución.
b. Se evalúan los impactos que pueden ocasionar la interrupción o indisponibilidad de cada uno de los servicios y sistemas de tecnología de información identificados.
c. Como parte del Plan de Contingencia se ha procedido a determinar los posibles riesgos e impactos en la Institución, donde se han considerado las siguientes áreas de impacto: operacional, legal, e imagen. A continuación, se muestra el Cuadro Nº 1: Descripción de Impactos.

Impacto	Áreas de Impacto		
	Operacional	**Legal**	**Imagen**
Leve	Paralización o trastornos en las actividades. El daño se revierte inmediatamente después de lo ocurrido.	-	Percepción negativa de la imagen institucional por un número reducido de usuarios finales.
Moderado	Paralización o trastornos en las actividades. El daño se revierte en un tiempo menor o igual al RTO.	Amonestación administrativa.	Percepción negativa de la imagen institucional por parte de las organizaciones políticas.
Alto	Paralización o trastornos en las actividades. El daño se revierte en un tiempo mayor al RTO.	Acciones judiciales, contenciosas, civiles.	Percepción negativa de la imagen institucional por parte de las organizaciones políticas y de las entidades públicas.
Severo	Paralización o trastornos en las actividades. El daño afecta totalmente la continuidad de las operaciones. El daño se revierte en un tiempo mayor al MTD.	Denuncias penales contra funcionarios del SERFOR.	Pérdida de la confianza y credibilidad de la institución por parte de la ciudadanía en general.

Cuadro N° 1: Descripción de Impactos

7.1. Descripción de los Eventos de Contingencias

TIPO		EVENTO	DESCRIPCIÓN
Externo	Tecnológico	Caída o interrupción de energía eléctrica - (E1)	Corresponde al corte del servicio de energía eléctrica en la Sede Central del SERFOR ubicado en Av. Javier Prado oeste 2442, corte eléctrico que genera interrupción del funcionamiento de los servidores donde se alojan los sistemas de información y/o aplicaciones del SERFOR. Esta situación impacta en la disponibilidad de los servicios de TI.
		Infección masiva por software malicioso – (E3)	Es el riesgo de infección de los equipos de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de las unidades de trabajo.
		Ataque informático (E12)	Consiste en aprovechar alguna debilidad o falla en el software o hardware, para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización.
	Operativo	Suspensión de las actividades por sismo, inundación o incendio – (E4)	Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo o incendio que afecte la infraestructura tecnológica del SERFOR generando suspensión total o parcial del funcionamiento del Centro de Datos o de la prestación de servicios de TI
	Técnico	Caída de internet – (E2)	Consiste en las fallas técnicas por parte del proveedor del servicio de internet en la Sede Central del SERFOR ubicado en Av. Javier Prado oeste 2442, lo que ocasionaría suspensión de los servicios de TI incluyendo correo, red, sistemas y aplicativos de información del SERFOR.
Interno	Tecnológico	Falla técnica en equipos servidores– (E6)	Corresponde al daño físico o lógico de un equipo servidor, que afecta el funcionamiento de un sistema de información crítico por falta de

TIPO		EVENTO	DESCRIPCIÓN
			mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o Inestable.
		Falla técnica en equipos de comunicación (E10)	Corresponde al daño físico o lógico de un equipo de comunicación, que afecta el funcionamiento de los servicios de información crítico por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o Inestable.
		Falla técnica en equipos de clientes clave (E11)	Corresponde al daño físico o lógico de un equipo cliente considerado clave para la entidad.
		Falla técnica en Sistemas de Información critico – (E7)	Representa una falla técnica en alguna funcionalidad de los sistemas de información y aplicativos críticos del SERFOR que se vea afectada la integridad de la información en el continuo uso de estos.
	Operativo	Accesos no autorizados al Centro de Datos del SERFOR – (E5)	Consiste en el acceso al Centro de Datos de personal no autorizadas que pueden ocasionar sabotaje, robo, alteración o extracción de información que es considerada confidencial o clasificada, así como también el daño a los componentes informáticos. El impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional.
		Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes – (E8)	Corresponde a la falta o inasistencia en un momento dado, de un trabajador crítico de la OTI que realiza actividades de soporte a usuarios sobre un sistema de información crítico del SERFOR por enfermedad, epidemia muerte o incapacidad, lo que genera inoperancia o inestabilidad de los sistemas de información, servidores y redes.

TIPO		EVENTO	DESCRIPCIÓN
	Técnico	Calentamiento del centro de datos – (E9)	Consiste en el aumento de temperatura dentro del centro de datos y falta de ventilación, por deficiencia del sistema de ventilación o ausencia de un sistema de ventilación de precisión acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos.

Cuadro N° 2: Descripción de Eventos

7.2. Valoración de los Eventos de Contingencia

La determinación del impacto, probabilidad y del evento de contingencia se realizarán según lo establecido en la Política de Seguridad de la Información del SERFOR

		PROBABILIDAD				
		Raro	Poco probable	Posible	Muy probable	Casi seguro
CONSECUENCIAS	Despreciable	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

Figura N° 2: Mapa de Calor de Riesgos (Fuente: Gestión de riesgos ISO 31000)

Para la valoración de los eventos identificados, se utiliza la matriz de la figura N° 1, donde se categorizan los niveles de probabilidad y niveles de impacto (consecuencias). La descripción de cada categoría se muestra a continuación:

Niveles de probabilidad

- Casi Seguro: probabilidad muy alta
- Muy probable: probabilidad alta
- Posible: probabilidad media
- Poco probable: probabilidad baja

- Raro: sería especialmente raro que ocurriera

Niveles de impacto (consecuencias)

- Catastrófico: pérdida de negocio o posibilidad de pérdida de vidas o lesiones graves
- Mayor: afección grave al negocio, posibilidad de lesiones moderadas
- Moderado: causarán problemas no significativos en el negocio, posibilidad de lesiones leves
- Menor: muy poca influencia sobre el negocio, impacto leve
- Despreciable: prácticamente ninguna influencia negativa sobre el negocio, pueden dejarse sin mediar

La valoración de los riesgos tiene 4 posibles resultados: bajo, medio, alto y muy alto. Para efectos de la formulación del presente plan de contingencia, se tomarán en cuenta los riesgos valorados como **alto y muy alto**. Los riesgos con valoración **bajo y medio** se deben mantener en lista de observación a fin de que de manera periódica se pueda evaluar si en el tiempo va cambiando dicha valoración.

En función a ello, los eventos de contingencia descritos en el numeral 7.2 precedente, tienen la siguiente valoración:

N°	EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN
E1	Caída o interrupción de energía eléctrica	Poco probable	Catastrófico	ALTO
E2	Caída de internet	Poco probable	Mayor	ALTO
E3	Infección masiva por software malicioso	Muy probable	Mayor	ALTO
E4	Suspensión de las actividades por sismo, inundación o incendio	Poco probable	Catastrófico	ALTO
E5	Accesos no autorizados al Centro de Datos del SERFOR	Poco probable	Mayor	MEDIO
E6	Falla técnica en equipos servidores, de escritorio o de comunicaciones	Posible	Mayor	ALTO
E7	Falla técnica en Sistemas de Información critico	Muy probable	Mayor	ALTO
E8	Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y	Muy probable	Moderado	ALTO

N°	EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN
	mantenimiento a los a los sistemas de información y comunicaciones			
E9	Calentamiento del centro de datos	Posible	Mayor	ALTO
E10	Falla técnica en equipos de comunicación	Posible	Mayor	ALTO
E11	Falla técnica en equipos de clientes clave	Posible	Mayor	ALTO
E12	Ataque informático	Muy probable	Mayor	ALTO

Cuadro N° 3: Valorización de riesgos

VIII. RESULTADOS ESPERADOS

8.1. El presente Plan de Contingencia de TI buscar restablecer los servicios de TI en un margen aceptable a cada tipo de servicio que pueden ir desde 50% hasta 100% dependiendo del tipo de servicio impactado.

IX. ESTRATEGIAS

9.1. Planes de Contingencia

Desarrollaremos las estrategias relacionadas con cada evento o incidente que provoque alto impacto en la continuidad de los servicios de TI de la OTI. Para lo cual se está dividiendo en 3 partes:

a. **Prevención:** Mecanismos para prevenir dichos eventos antes de que sucedan; ayudan a reducir el impacto y estar siempre preparados ante eventualidades de desastres.
b. **Ejecución:** Después de iniciado el evento y ayuda a la recuperación de las funciones críticas, se considera los tiempos de continuidad.
c. **Recuperación:** Procedimientos para retomar las actividades ya recuperadas en su lugar de origen.

SERFOR	Evento: Caída o interrupción de energía eléctrica - (E1)	OTI
1. PLAN DE PREVENCIÓN		
1.1. Descripción del evento Falla general del suministro de energía eléctrica por parte del proveedor de servicios y fallo y/o no disponibilidad del grupo electrógeno. Este		

SERFOR	Evento: Caída o interrupción de energía eléctrica - (E1)	OTI

evento incluye los siguientes elementos mínimos identificados por el SERFOR, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

- Servicios Públicos
- Suministro de Energía Eléctrica
- Hardware
- Servidores
- Estaciones de Trabajo
- Equipos Diversos
- UPS

1.2. Objetivo

Restablecer energía eléctrica en el Centro de Datos del SERFOR ante un evento de contingencia para asegurar la continuidad operativa de los sistemas críticos de TI.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se delimita al Centro de Datos ubicado de la sede Central del SERFOR.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Verificar que durante las operaciones diarias de servicio u operaciones del SERFOR se contará con los UPS necesarios para asegurar el suministro eléctrico en el Centro de Datos del SERFOR.
- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 45 minutos como mínimo.
- Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

Corte de suministro de energía en la Sede Central del SERFOR por un tiempo mayor a 30 minutos.

2.2. Procesos relacionados antes del evento

SERFOR	Evento: Caída o interrupción de energía eléctrica - (E1)	OTI

Cualquier actividad de servicio dentro de las instalaciones de la sede principal del SERFOR.

2.3. Personal que autoriza la Contingencia

- Jefa o jefe de la Oficina de Tecnologías de la Información.

2.4. Personal encargado

- Especialista en administración de Data Center o quien haga sus veces.

2.5. Descripción de los procedimientos después de activar la contingencia:

- Informar a la Jefatura de la Oficina de Tecnologías de la Información sobre el evento presentado.
- Verificar la activación automática de los UPS.
- Comunicar a todas las Unidades Orgánicas del SERFOR del evento y coordinar las acciones necesarias.
- En caso la interrupción de energía sea mayor a 30 minutos se deberá apagar los servidores (Virtuales y físicos) que alojen los sistemas, aplicaciones, servicios de TI y demás servidores en siguiente orden:
    - Servidores de aplicación, Base de datos, servicios TI, otros, servicio de Directorio Activo y finalmente los servidores físicos (Hypervisores)
    - Apagar los servicios los equipos de seguridad perimetral y comunicaciones.

- Monitorear el uso de equipos UPS para el restablecimiento de energía en los servidores de soporte a los sistemas críticos.

- Coordinar con las Unidades Orgánicas afectadas de tomar las medidas necesarias ante la activación del Plan de Contingencia de TI.

3. PLAN DE RECUPERACIÓN

3.1. Personal operativo encargado

- Especialista de administración de Data Center o quien haga sus veces
- Especialista en redes y comunicaciones
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades

- Verificar el estado de la infraestructura tecnológica impactada por el evento.
- Verifica el restablecimiento de la energía eléctrica y el funcionamiento del Centro de Datos.

SERFOR	Evento: Caída o interrupción de energía eléctrica - (E1)	OTI

- En caso de que se cuente con energía eléctrica, se procederá la activación de los servicios en la siguiente secuencia:
  - Encendido de los equipos de seguridad perimetral y comunicaciones.
  - Encendido de los servidores físicos (Hypervisores)
  - Encender servidores de Directorio Activo, Base de datos, Aplicaciones, otros.
- Analizar la necesidad de usar las copias de respaldo y backups.
- Verificar el restablecimiento de los sistemas críticos de información.
- Comunicar a las Unidades Orgánicas afectadas el restablecimiento de los sistemas de información críticos
- Registrar aquellas actividades que sirva para actualizar el Plan de Contingencia de TI en caso vuelva a presentarse dicha eventualidad.
- Registrar el evento en el Formato Registro de Contingencias

3.3. Mecanismo de comprobación

- Verificar a través del software de Monitoreo que todos los servicios estén activos
- Comunicar a todas las Unidades Orgánicas del SERFOR a fin de constatar el correcto funcionamiento de los sistemas de información críticos en cada Oficina de trabajo.
- Garantizar la funcionalidad de las instalaciones eléctricas en la Sede Central del SERFOR.

3.4. Desactivación del Plan de Contingencia de TI

La Jefa o Jefe de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez se haya restablecido la energía eléctrica al Centro de Datos y los servicios de TI.

3.5. Informe de resultados

Elaborar un informe a la Jefatura de la Oficina de Tecnologías de la Información sobre el problema presentado y el procedimiento usado para atender el evento.

3.6. Proceso de actualización del Plan

Se tomarán las recomendaciones formuladas en los informes presentados a la Jefatura de la Oficina de Tecnologías de la Información para la presente contingencia.

3.7. Tiempo de Recuperación

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica. Para el restablecimiento de la operación del grupo electrógeno se estima un tiempo máximo de ½ hora.

SERFOR	Evento: Caída de Internet – (E2)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Perdida de servicio de Internet a la conexión de la red externa del servicio principal de SERFOR.

1.2. Objetivo

Restaurar los servicios críticos de comunicaciones a la red externa que soportan los servidores del Centro de Datos a través del Servicio de Internet de Contingencia.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se puede producir durante el servicio, o en horario no laborable en el Centro de Datos del SERFOR.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en Redes y Comunicaciones o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Contar con equipos de comunicación y respaldo ante posibles fallas del router principal, a través del contrato con el proveedor del servicio de Internet se contempla el reemplazo del router en caso falle.
- Contar con mantenimiento preventivo para los equipos de comunicaciones dos veces al año. (Equipo alquilado) y otro mantenimiento programado por el proveedor en su nodo de comunicaciones.
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Falla del sistema de router principal para el servicio de Internet
- Falla de los circuitos digitales de comunicación de red externa. (Ej. Rotura de enlace de fibra u otros medios)
- Falla del nodo de comunicación del proveedor de internet del SERFOR

2.2. Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones del SERFOR.

2.3. Personal que autoriza la Contingencia

- Jefa o Jefe de la Oficina de Tecnologías de la Información del SERFOR.

SERFOR	Evento: Caída de Internet – (E2)	OTI

2.4. Personal encargado
- Especialista en Redes y Comunicaciones o quien haga sus veces

2.5. Descripción de los procedimientos después de activar la contingencia:
- Verificar la magnitud del fallo o avería al sistema de comunicación a la red externa (Internet)
- Notificar al proveedor de Servicios de Internet sobre la magnitud de fallos o avería. (Ej. Estado de router, enlaces, etc.)
- El proveedor toma control para descartar si es un problema interno. Si es falla del Router el proveedor procede con el cambio. (Max. 1hora)
- En caso de que la falla sea el circuito de comunicaciones, el proveedor se encarga de solucionar el problema de acuerdos a los SLAs comprometidos.
- El proveedor notifica la solución con un informe de la incidencia presentada
- Validar que los servicios se encuentren en línea a través de la herramienta de Monitoreo.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
- Oficial de seguridad de la información.
- Especialista en Redes y Comunicaciones o quien haga sus veces

3.2. Descripción de actividades
- Validar que los servicios y circuitos estén conforme por las áreas usuarias.
- El proveedor del servicio de Internet una vez reparado el fallo emitirá un informe a la Jefatura de Tecnologías de la Información, detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Información sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación
La OTI deberá asegurarse que las pruebas y revisiones periódicas al sistema de comunicaciones y circuiros de la red externa (Internet), los cuales se lleven a cabo semestralmente.

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

SERFOR	Evento: Caída de Internet – (E2)	OTI

3.5. Proceso de actualización
En base al informe presentado por el proveedor del sistema de comunicaciones y circuitos de red externa (Internet), se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de Recuperación
- Falla del Router: El reemplazo por el proveedor no debe exceder a 1 hora.
- Falla de Circuito digital: El tiempo del SLA establecido con el proveedor es 4 horas.

SERFOR	Evento: Infección masiva por software malicioso – (E3)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Los softwares maliciosos son programas informáticos que se propagan de un equipo a otro y que interfieren en su correcto funcionamiento. Además, pueden dañar o eliminar los datos de un equipo. Este evento incluye los siguientes elementos mínimos identificados por el SERFOR, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:
- Servidores
- Estaciones de trabajo (PC y Laptops)
- Software base datos.
- Aplicativos y sistemas de información del SERFOR.

1.2. Objetivo
Restaurar la operatividad de los activos informáticos después de eliminar el software malicioso que causa la contingencia.

1.3. Valoración
Este evento es considerado alto.

1.4. Entorno
Los activos informáticos (PC, Laptops, servidores y sistemas de información) de la Sede Central del SERFOR.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Soporte Técnico o quien haga sus veces.

1.6. Condiciones de prevención de riesgos

SERFOR	Evento: Infección masiva por software malicioso – (E3)	OTI

- Establecer políticas y normativas de seguridad que regulen el uso adecuado de los activos de información
- Utilizar mecanismos de seguridad que restrinja el acceso a páginas de internet de contenido malicioso.
- Restringir el acceso a las grabadoras de CD y USB en las estaciones de trabajo que no lo requieran.
- Aplicar filtros para restricción de correo entrante y así prevenir la infección de los terminales de trabajo por virus.
- Verificar que el antivirus instalado en cada estación de trabajo deba estar actualizado permanentemente.
- Verificar que los sistemas operativos cuenten con los parches de actualización constantemente, a través de la herramienta WSUS la cual debe estar operativa.
- Escanear la red constantemente a fin de identificar instalaciones de agentes maliciosos.
- Contar con un mínimo de tres equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta la operatividad del equipo cliente afectado.
- Capacitar y concientizar al personal del SERFOR sobre temas de seguridad de la información.
- Contar con Backups y copias de respaldo de la información
- Encriptación de los datos críticos
- Segmentar la red para asilar los casos de activos infectados por Malware o software malicioso.
- Controlar el nivel de obsolescencia tecnológica aceptable a nivel Hardware y Software

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Mensajes de error o mensajes de alerta durante la ejecución de los sistemas de información y aplicaciones.
- Lentitud o paralización de los sistemas de información y aplicaciones.
- Falla general en los activos de informáticos (PC, Laptops, servidores y sistemas de información).
- Reporte de usuarios.

2.2. Procesos relacionados antes del evento

Cualquier proceso relacionado con el uso de sistemas y aplicaciones en las. estaciones de trabajo y servidores

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información.

2.4. Personal encargado

SERFOR	Evento: Infección masiva por software malicioso – (E3)	OTI

- Especialista en administración de Data Center o quien haga sus veces.
- Soporte técnico o quien haga sus veces.

2.5. Descripción de actividades

- Comunicar o escalar a Jefa o Jefe de OTI para activar al equipo de respuesta de incidentes.
- Desconectar preventivamente los equipos infectados de la red de SERFOR.
- Comunicar a los usuarios de los servicios de los equipos impactados.
- Verificar el estado actualizado de las firmas del software antivirus, IPS, Antimalware
- Verificar la infección de los equipos afectado y el alcance de este.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.) para su remisión y revisión por el fabricante de la solución antivirus y antimalware.
- Eliminar el agente viral causante de la infección.
- Escanear la red del SERFOR en virtud de eliminar posibles agentes virales informáticos.
- En caso no solucionarse el problema:
  - Formatear el equipo
  - Personalizar la estación para el usuario.
- Conectar las estaciones o equipo servidor a la red del SERFOR.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en la administración de Data Center o quien haga sus veces
- Especialista en redes y comunicaciones o quien haga sus veces.
- Soporte técnico o quien haga sus veces.

3.2. Descripción de actividades

- Registrar la conformidad del usuario una vez se haya eliminado la amenaza de virus en su estación de trabajo.
- Realizar pruebas de funcionamiento en las estaciones de trabajo (Sistemas de información, servicios tecnológicos y aplicaciones del SERFOR).
- Coordinar con el usuario responsable el procedimiento para reanudar las labores normales en el ambiente de trabajo original.
- Dar indicaciones de seguridad y prevención a los usuarios.
- Recomendar capacitación a la OTI de ser necesario

SERFOR	Evento: Infección masiva por software malicioso – (E3)	OTI

- Realizar informe de las acciones tomadas durante el evento.

Se informará a la Jefatura de la Oficina de Tecnología de la Información el tipo de software malicioso encontrado y el procedimiento usado para removerlo. En función a esto, se tomarán las medidas preventivas del caso. El evento será evaluado y registrado en el formato de registro de contingencia.

3.3. Mecanismo de comprobación

- Asegurar que el antivirus funcione correctamente y se encuentre en constante actualización.
- Verificar que el Sistema Operativo se encuentre con las actualizaciones y parches.

3.4. Desactivación del plan de continuidad

La jefa o Jefe de la Oficina de Tecnologías de la Información desactivará el presente Plan una vez se haya eliminado la amenaza.

3.5. Proceso de actualización

En base al informe presentado que identifica las causas de la infección de virus informático, se determinará las acciones preventivas necesarias que deberán incluirse en el presente Plan.

3.6. Tiempo de Recuperación

La duración del evento dependerá de la eficacia en detección de infección masiva, por efecto de actualización de firmas no mayor a 24 horas, así como también el tiempo de respuesta de los fabricantes en caso infecciones de día Cero.

Los usuarios deberán esperar las indicaciones del personal de soporte para reanudar el trabajo.

SERFOR	Evento: Suspensión de las actividades por sismo, inundación o incendio – (E4)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Constituye la situación en la que el Centro de Datos del SERFOR se encuentra declarada inhabitable, producto de un desastre de mayores magnitudes, pudiendo provocar derrumbe de la infraestructura, perdida de materiales, recursos informáticos y humanos.

Las causas que pueden provocar este evento encontramos las siguientes:

SERFOR	Evento: Suspensión de las actividades por sismo, inundación o incendio – (E4)	OTI

Incendio: Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.

Sismo de gran intensidad en Lima: Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento errático del terreno.

Inundación: Flujo descontrolado de agua producto de lluvias torrenciales o fugas y/o daños en el sistema hidráulico.

1.2. Objetivo

Establecer las acciones que se tomarán ante un incendio, inundación o sismo de grandes magnitudes a fin de minimizar el tiempo de interrupción de los servicios críticos de TI, establecidos en el numeral 6.3 cuadro de valoración de Alto y Muy Alto

1.3. Valoración

Este evento es considerado como alto.

1.4. Entorno

Este evento se localiza en las instalaciones del Centro de Datos de la sede central del SERFOR.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.
- Especialista de Base de Datos
- Especialistas de Desarrollo

1.6. Condiciones de prevención de riesgos

Incendio de grandes magnitudes en uno o más ambientes:

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Asistir a charlas sobre el uso y manejo de extintores de cada uno de los tipos.
- Acatar las indicaciones de Defensa Civil, en torno al evento.

SERFOR	Evento: Suspensión de las actividades por sismo, inundación o incendio – (E4)	OTI

- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal responsable de las acciones de prevención y ejecución de la contingencia.
- Verificar el funcionamiento de los detectores de humo en el Centro de Datos del SERFOR.
- Contar con una lista de contactos de las personas responsables y proveedores de servicios de contingencia.
- Conocer el grupo de brigadistas asignados por el SERFOR.
- Identificar la ubicación de las estaciones manuales de alarma contra incendio.

Sismo de gran intensidad en Lima

- Solicitar el plan de evacuación de las instalaciones del SERFOR, el mismo que debe ser de conocimiento de todo el personal que labora.
- Participar en los simulacros de evacuación con la participación de todo el personal del SERFOR.
- Mantener las salidas libres de obstáculos en Centro de Datos
- Señalizar todas las salidas del Centro de Datos
- Señalizar las zonas seguras del Centro de Datos
- Contar con una lista de contactos de las personas responsables y proveedores de servicios de contingencia.
- Conocer el grupo de brigadistas asignados por el SERFOR.

Inundaciones de grandes magnitudes

- Solicitar a Servicios Generales la coordinación del mantenimiento y/o estado de las instalaciones hidráulicas del SERFOR.
- Posicionar los activos estratégicos del Centro de Datos en plataformas elevadas.
- Contar con una lista de contactos de las personas responsables y proveedores de servicios de contingencia.
- Conocer el grupo de brigadistas asignados por el SERFOR.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

El proceso de contingencia se activará inmediatamente después de ocurrido los eventos descritos en el numeral 1.1.

2.2. Personal que autoriza la Contingencia

La Jefatura de la Oficina de Tecnologías de la Información con la autorización de la Dirección ejecutiva del SERFOR.

2.3. Personal encargado Operativo

- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.

SERFOR	Evento: Suspensión de las actividades por sismo, inundación o incendio – (E4)	OTI

- Administrador de base de datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.
- Web Master o quien haga sus veces.

2.4. Descripción de actividades para la restauración del Centro de Datos

- Evaluar los daños ocasionados en el Centro de Datos del SERFOR.
- Verificar la disponibilidad del espacio físico que hará las veces de Centro de Datos alterno provisional del SERFOR, en caso de inoperancia del Centro de Datos Principal.
- Trasladar el equipamiento que se encuentre en buenas condiciones del Centro de Datos, asegurando que las características ambientales sean las mínimas necesarias para su implementación.
- Asegurar las condiciones eléctricas y de refrigeración mínimas para el funcionamiento del Centro de Datos alterno provisional.
- Considerar la adquisición de equipamiento tecnológico que asegure la disponibilidad del Centro de Datos provisional.
- Configurar la infraestructura tecnológica que soporte el levantamiento de los sistemas de información críticos del SERFOR.
- Coordinar el traslado seguro de las copias de seguridad en custodia por el proveedor al nuevo ambiente de físico del Centro de Datos provisional.
- Restaurar las copias de seguridad de los sistemas de información del SERFOR.
- Ejecutar las pruebas necesarias para asegurar la disponibilidad de los servicios críticos de TI.
- Informar a la Jefatura de la Oficina de Tecnologías de la Información el restablecimiento del Centro de Datos alterno provisional del SERFOR.
- Instalación de los servicios Internet y enlace de datos a RENIEC

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.
- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.
- Web Master o quien haga sus veces.

3.2. Descripción de actividades

- Verificar los daños a los componentes informáticos del Centro de Datos principal.
- Realizar el inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de estos.

SERFOR	Evento: Suspensión de las actividades por sismo, inundación o incendio – (E4)	OTI

- Trasladar hacia el Centro de Datos alterno provisional los componentes informáticos en buen estado.
- Habilitar los muebles y logística necesaria para su operatividad.
- Garantizar la habilitación del servicio de fluido eléctrico.
- Reinstalación del personal critico de TI.
- Monitorear constantemente la funcionalidad de los servicios críticos de TI.

3.3. Mecanismo de comprobación

Elaborar un informe a la Jefatura de Tecnologías de la Información detallando los daños afectados a los activos de Información críticos del SERFOR y las acciones tomadas.
Se llenará el formato de ocurrencia de eventos para este fin.

3.4. Desactivación del Plan de Recuperación

Se desactivará una vez se tome por superado el desastre y se retome las actividades de origen.

3.5. Proceso de actualización

El proceso de actualización será en base al informe presentado a la Dirección Ejecutiva a efectos que determine las acciones a tomar.

3.6. Tiempo de Recuperación

El proceso de implementar un Centro de Datos provisional (de ser necesario) tomara un tiempo no mayor a 5 días.

La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

SERFOR	Evento: Falla técnica en servidores – (E6)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Falla técnica de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del SERFOR.

1.2. Objetivo

Asegurar la continuidad y operatividad de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del SERFOR.

1.3. Valoración

SERFOR	Evento: Falla técnica en servidores – (E6)	OTI

Este evento es considerado alto.

1.4. Entorno

Servidores de soporte para los servicios críticos de TI, sistemas de información y aplicaciones localizados en el Centro de Datos del SERFOR.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Revisión periódica técnica de los servidores del Centro de Datos.
- Mantener actualizada la garantía de equipos y servidores vigentes.
- Copias de seguridad de los sistemas de información y aplicaciones del SERFOR.
- Monitoreo periódico de red del SERFOR.
- Seguridad periférica.
- Protección física adecuada al Centro de Datos.
- Mecanismos de seguridad y controles de acceso.
- Adecuada ventilación y refrigeración en el Centro de Datos.
- Procedimientos para el uso correctos de los activos de información.

1.7. Copias de respaldo o Backup y custodia en una locación externa.

- Tener las copias de respaldo de información disponibles para su aplicación en los servidores de contingencia del SERFOR.
- Traslado de las copias de seguridad en poder del proveedor de custodia a la Sede Central del SERFOR.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Fallas en la conexión, servidores no responden.
- Indisponibilidad de uso de los sistemas y aplicativos del SERFOR.

2.2. Personal encargado

- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

2.3. Descripción de los procedimientos después de activar la contingencia:

- Analizar la causa resultante o disparador del evento.

SERFOR	Evento: Falla técnica en servidores – (E6)	OTI

- Realizar un diagnóstico rápido de los sistemas críticos afectados o involucrados en la ejecución. Para este caso se debe revisar el inventario de los sistemas o aplicaciones críticas del SERFOR.
- Contactar a las partes interesadas que sean afectadas por la indisponibilidad de los servicios de TI.
- Comunicar a los proveedores del equipo servidor e informar la incidencia como parte del soporte y garantía.
- Desconectar de la red el servidor afectado.
- Activar y configurar el equipo necesario de contingencia para el levantamiento de los servicios de TI en los servidores alternos de contingencia.
- Ejecutar las restauraciones de los backups de los sistemas y aplicaciones críticos en los servidores alternos de contingencia en caso se requiera.
- Realizar las pruebas de funcionamiento.
- Comunicar a los usuarios el restablecimiento de los servicios de TI.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Centro de Datos.
- Especialista en redes y comunicaciones.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades

- Conectar a la red el equipo inicial reparado.
- El Especialista en Administración de Centro de Datos verifica el correcto desempeño de los servidores reparados y de los sistemas de información críticos que soportan.
- Se informará a la Jefatura de Oficina de Tecnologías de la Información la causa del problema presentado y el procedimiento usado para atender el problema. En función a esto, se tomarán las medidas preventivas del caso.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

3.3. Mecanismos de Comprobación

- Una vez identificada el origen de la falla de los servidores que ocasionó el evento, se deberá realizar un informe técnico detallado y consolidando las acciones tomadas.
- Revisar las configuraciones y programar con el proveedor de los equipos, revisiones periódicas a fin de reducir la amenaza que vuelva a suceder.

SERFOR	Evento: Falla técnica en servidores – (E6)	OTI

3.4. Desactivación del Plan de Contingencia
Jefa o Jefe de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que el especialista en administración de Data Center informe la operatividad de los servidores.

3.5. Proceso de actualización
El proceso de actualización será en base al informe presentado a la Dirección Ejecutiva quien determinará las acciones a tomar.

3.6. Tiempo de Recuperación
Duración de 4-8 horas.

SERFOR	Evento: Falla en Sistemas de Información Críticos – (E7)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Es el uso defectuoso de los sistemas de información críticos del SERFOR, haciendo que el uso de estos corresponda a un elevado riesgo en la integridad de la información que se procese o simplemente este último deje de funcionar.

1.2. Objetivo
Restaurar el funcionamiento de los sistemas de información y aplicaciones críticos del SERFOR de acuerdo con el numeral 6.3 cuadro de valoración de Alto y Muy Alto.

1.3. Valoración
Este evento es considerado alto.

1.4. Entorno
Sistemas de información y aplicativos críticos del SERFOR.

1.5. Personal encargado
- Oficial de seguridad de la información
- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo
- Copia de seguridad de la información críticos para asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos relacionadas.
- Mantener actualizado el software de gestión de BD, con todos los parches del producto según el fabricante y licencias vigentes.

SERFOR	Evento: Falla en Sistemas de Información Críticos – (E7)	OTI

- Evitar el uso de software no licenciado que pueda estar corrupto
- Revisión preventiva de los sistemas y mantenimiento general de las bases de datos.
- Directivas o procedimiento de desarrollo seguro.
- Implementar y mantener un repositorio de código fuente institucional

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

Fallas en el uso de los sistemas de información que generen su inoperatividad.

Información procesada no cuenta con integridad y fiabilidad.

2.2. Procesos relacionados antes del evento

Respaldo disponible de los sistemas de información críticos.

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información del SERFOR.

2.4. Personal encargado

- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.

2.5. Descripción de las actividades después de activar la contingencia:

- Desconectar de la red el equipo afectado.
- Configurar equipo de respaldo para el sistema de información o aplicación crítica afectada.
- Restaurar la copia de seguridad más reciente del aplicativo crítico correspondiente.
- Crear los permisos a cada carpeta compartida.
- Verificar la existencia del servidor nuevo en el dominio y colocarlo en producción.

Informar a los usuarios la nueva ruta del servidor del aplicativo

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Centro de Datos.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades

- Revisar el sistema de Información o aplicativo dañado para determinar la falla o error lógico presentado.
- Hacer pruebas al sistema de Información o aplicativo una vez entregada la solución por el proveedor, en ambiente de pruebas.

SERFOR	Evento: Falla en Sistemas de Información Críticos – (E7)	OTI

- Realizar copia de la base de datos del sistema de Información o aplicativo que está en funcionamiento como contingencia.
- Restaurar la copia de seguridad más reciente del aplicativo afectado en el servidor inicial.
- Verificar los permisos sobre el sistema de información o aplicativo.
- Informar a los usuarios la ruta del servidor del sistema de información o aplicativo.
- Conectar a la red el equipo inicial reparado.

3.3. Mecanismos de comprobación

El Especialista en administración de Centro de Datos presentara un informe a la Jefatura de la Oficina de Tecnologías de la Información explicando que servicio ha sido afectado y cual son las acciones tomadas.

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.

3.5. Proceso de actualización

En base al informe presentado a la Jefatura de Oficina de Tecnologías de la información y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

3.6. Tiempo de Recuperación

El tiempo máximo de duración de la contingencia será máximo en 24 horas dependiendo de la causa que originó la contingencia.

SERFOR	Evento: Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes– (E8)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Ausencias del personal (enfermedad, epidemias, renuncias masivas, ceses), critico que brinda soporte y mantenimiento a los sistemas de información, servidores y redes que mediante su ausencia pueda originar paralización en las operaciones del SERFOR.

1.2. Objetivo

Reemplazar al personal crítico ausente con elementos capacitados que puedan cubrir sus funciones hasta la inserción o reemplazo del ausente.

SERFOR	Evento: Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes– (E8)	OTI

1.3. Valoración
Este evento es considerado Alto.

1.4. Entorno
Oficina de Tecnologías de la Información.

1.5. Personal encargado
- Jefa o Jefe de la Oficina de Tecnologías de la Información.
- Oficial de seguridad de la información.

1.6. Condiciones de Prevención de Riesgo
- Asegurar la capacitación adecuada de los equipos técnicos en su especialidad, Analistas de sistemas, redes, infraestructura y Seguridad Informática y Administración de BD con el fin de que cumplan con el perfil, conocimiento y capacidad de reemplazar la ausencia de los especialistas en caso de ausencia.
- Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labor.
- Elaborar diccionarios de datos y/o manuales o procedimientos operativos de uso para facilitar las actividades del reemplazante.
- Programar chequeos preventivos médicos al personal crítico en periodos semestrales o anuales.
- Mantener operativas las herramientas de trabajo remoto.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
Inasistencia no premeditada del personal crítico (administrador de sistemas y redes).

2.2. Procesos relacionados antes del evento
La Jefatura de la Oficina de Tecnologías de la Información tiene conocimiento de inasistencia del personal crítico.

2.3. Personal que autoriza la Contingencia
- Jefa o Jefe de la Oficina de Tecnologías de la Información del SERFOR.

2.4. Personal encargado
- Jefa o Jefe de la Oficina de Tecnologías de la Información.
- Oficial de seguridad de la información.

2.5. Descripción de las actividades después de activar la contingencia:

SERFOR	Evento: Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes– (E8)	OTI

- Confirmada la inasistencia del personal, la Jefatura de la Oficina de Tecnologías de la Información asignara al reemplazo provisional del personal ausente.
- Poner a disposición los recursos necesarios para que el personal suplente lleve a cabo sus actividades efectivamente.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
Jefa o Jefe de la Oficina de Tecnologías de la Información

3.2. Descripción de actividades
- Facilitar la reinserción del personal ausente
- Regularización en los servicios pendiente durante la ausencia.
- Revisión de los servicios atendidos si fuera el caso.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

3.3. Mecanismos de comprobación
Informes de desempeño laboral cuando sea requerido por la Jefatura de la Oficina de Tecnologías de la Información

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.

3.5. Proceso de actualización
En base al informe presentado a la Jefatura de Oficina de Tecnologías de la información y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

3.6. Tiempo de Recuperación
El tiempo máximo de duración de la contingencia dependerá de la causa que originó la ausencia temporal, sin embargo se dispondrá de un reemplazo temporal en un plazo máximo de 24 horas.

SERFOR	Evento: Calentamiento del Centro de Datos – (E9)	OTI

1. PLAN DE PREVENCIÓN

SERFOR	Evento: Calentamiento del Centro de Datos – (E9)	OTI

1.1. Descripción del evento
Aumento de temperatura dentro del Centro de Datos y falta de sistema de aire acondicionado, en el centro de datos de SERFOR o ausencia de un sistema de ventilación acorde a las necesidades del SERFOR.

1.2. Objetivo
Restaurar los servicios críticos de TI que soportan los servidores del Centro de Datos.

1.3. Valoración
Este evento es considerado alto.

1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en el Centro de Datos del SERFOR.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo
- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con un sistema de aire acondicionado adecuado en el Centro de Datos.
- Contar con mantenimiento preventivo para los equipos de aire acondicionado.
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
- Falla del sistema de aire acondicionado del Centro de Datos
- Falla de los servicios críticos del SERFOR

2.2. Procesos relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones del SERFOR.

2.3. Personal que autoriza la Contingencia
- Jefa o Jefe de la Oficina de Tecnologías de la Información del SERFOR.

2.4. Personal encargado
- Especialista en administración de Data Center o quien haga sus veces.

2.5. Descripción de los procedimientos después de activar la contingencia:

SERFOR	Evento: Calentamiento del Centro de Datos – (E9)	OTI

- Verificar la magnitud del fallo o avería al sistema de ventilación del Centro de Datos.
- Notificar al proveedor de aire acondicionado sobre la magnitud de fallos o avería.
- Encender el aire acondicionado de contingencia.
- Instalar equipos de ventilación provisionales.
- Apagar los equipos electrónicos no críticos
- Restablecer el sistema de aire acondicionado del Centro de Datos.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Especialista en administración de Data Center o quien haga sus veces.

3.2. Descripción de actividades

- El especialista de administración de Data Center revisara que el sistema de Aire Acondicionado haya sido reparado y funcione con normalidad.
- Encender equipos no críticos
- El proveedor del sistema de aire acondicionado una vez reparado el fallo emitirá un informe a la Jefatura de Tecnologías de la Información, detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Información sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La OTI deberá asegurarse que las pruebas y revisiones periódicas al sistema de ventilación del Centro de Datos se lleven a cabo semestralmente.

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización

En base al informe presentado por el proveedor del sistema de ventilación de Centro de Datos se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de Recuperación

El tiempo máximo de duración de la contingencia dependerá del proveedor del sistema del aire acondicionado, se estima un tiempo máximo de 2 horas.

SERFOR	Evento: Falla técnica de equipos de Comunicación – (E10)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Caída de los equipos de comunicación (Switches) o fallas en los enlaces de fibra en la sede central. (Principal o redundante)

1.2. Objetivo

Restaurar los servicios críticos de comunicaciones de la red interna que soportan los Sistemas de SERFOR.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se puede producir durante el servicio, o en horario no laborable en el Centro de Datos del SERFOR.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en redes y comunicaciones o quien haga sus veces

1.6. Condiciones de Prevención de Riesgo

- Contar con equipo en configuración redundante y alta disponibilidad.
- Contar con equipos de Switches de respaldo ante posibles fallas de los equipos de comunicación.
- Enlaces redundantes entre equipos de comunicación a nivel de Switch Core
- Los Switches de distribución también estarían en configuración redundante.
- Los Switches de acceso que conecta a las PCs, se cuenta con equipos de respaldo.
- Contar con mantenimiento preventivo para los equipos de comunicación (Switch Core y Distribución).
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Falla del Switchs Core, Distribución y acceso a las PCs
- Falla de los enlaces de cobre o fibra en la red interna.

2.2. Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones del SERFOR.

SERFOR	Evento: Falla técnica de equipos de Comunicación – (E10)	OTI

2.3. Personal que autoriza la Contingencia
- Jefa o Jefe de la Oficina de Tecnologías de la Información del SERFOR.

2.4. Personal encargado
- Especialista en Redes y Comunicaciones o quien haga sus veces

2.5. Descripción de los procedimientos después de activar la contingencia:
- Validación física de la caída de red y dimensionar el alcance del impacto (Usuarios y pisos afectados)
- Si se trata un Switchs de acceso se reemplaza en caso este en garantía, caso contrario se envía a reparación el equipo de comunicación que presenta fallas.
- Se valida el estado de los servicios por usuarios y pisos afectado.
- Si trata de fallas en los enlaces, se verifica con la herramienta de monitoreo los estados y alertas reportadas.
- Se realiza una validación física de las conexiones de fibra (Cuarto de comunicaciones), si implica algún cambio se notifica al proveedor.
- El proveedor realiza un diagnóstico para detectar falla y proceder con su reparación.
- Se valida que los servicios en la herramienta de monitoreo estén activos para los usuarios y pisos afectados.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado
- Oficial de seguridad de la información.
- Especialista en Redes y Comunicaciones o quien haga sus veces

3.2. Descripción de actividades
- Validar que los equipos de comunicación y enlace de la red interna estén activos para las áreas usuarias.
- El proveedor de los equipos de comunicaciones una vez reparado el fallo emitirá un informe a la Jefatura de Tecnologías de la Información, detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Información sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La OTI deberá asegurarse que las pruebas y revisiones periódicas al sistema de comunicaciones de la red interna se lleven a cabo semestralmente (Equipos en garantía)

SERFOR	Evento: Falla técnica de equipos de Comunicación – (E10)	OTI

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización
En base al informe presentado por el proveedor del sistema de comunicaciones y circuitos de red interna se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de recuperación
- Falla de switches Core y Distribución, el tiempo máximo de reemplazo por el proveedor será de 1 hora.
- Switchs de accesos PCs máx. 1 hora.
- En caso falla de enlace digital dependerá de los SLAs del proveedor, se estima máximos 24 horas.

SERFOR	Evento: Falla técnica de equipos de Clientes Clave – (E11)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Corresponde al daño físico o lógico de un equipo cliente considerado clave para la entidad.

1.2. Objetivo
Restaurar los equipos de clientes críticos que soportan los servicios digitales de SERFOR.

1.3. Valoración
Este evento es considerado alto.

1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en el Centro de Datos del SERFOR.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo
- El control de los equipos informáticos está a cargo del área de Patrimonio

SERFOR	Evento: Falla técnica de equipos de Clientes Clave – (E11)	OTI

- Identificar e informar los equipos informáticos obsoletos (Desde año 2015).
- Mantenimiento anual en los equipos informático en todas las ATFFS.
- Equipos fuera de garantía, se coordina con al área de Patrimonio.
- Evaluación del estado del parque informático y priorizar la compra para nuevos equipos
- Contar con mantenimiento preventivo para los equipos informáticos
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

Falla de los equipos informáticos que soportan usuarios o áreas críticas.

2.2. Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones del SERFOR.

2.3. Personal que autoriza la Contingencia

- Jefa o Jefe de la Oficina de Tecnologías de la Información del SERFOR.

2.4. Personal encargado

- Especialista de Soporte Técnico de OTI o quien haga sus veces.

2.5. Descripción de los procedimientos después de activar la contingencia:

- Solicitar a Patrimonio si cuenta con stock de equipos informáticos (Equipos usados o nuevos)
- Dependerá de la incidencia reportada, se realiza una verificación al equipo asignado para su diagnóstico y solución.
- Preparar los equipos de cómputo para su remplazo al usuario(s) afectados.
- Notificas al área de Patrimonio, al usuario(a), Director(a) general, respecto a las actividades y atención realizada.
- Solicitar conformidad de la atención.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista de Soporte Técnico de OTI o quien haga sus veces.

3.2. Descripción de actividades

- Si la falla el equipo informático, se verifica si cuenta con garantía para contactar al proveedor para su solución.
- Si no se encuentra en garantía, se solicitan al área de Patrimonio otro equipo de reemplazo.

SERFOR	Evento: Falla técnica de equipos de Clientes Clave – (E11)	OTI

- Se preparan y prueban los equipos de reemplazo asignados antes de su reasignación.
- El proveedor de equipos informático una vez reparado el fallo emitirá un informe a la Jefatura de Tecnologías de la Información, detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Información, Oficial de Seguridad de la Información, Jefatura del área usuaria y Oficina de Abastecimiento, sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La OTI deberá asegurarse que las revisiones periódicas de los equipos informáticos se realizan una vez al año.

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización

En base al informe presentado por el proveedor de los equipos informáticos se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de recuperación

- Fallas de equipos informáticos: Tiempo máximo de respuesta es 24 horas
- Los tiempos de respuesta del proveedor depende de su stock (Pieza de recambio), se estima un tiempo de respuesta máximo de 3 días.

SERFOR	Evento: Ataque Informático – (E12)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Afectación por parte de algún sistema informático de un tipo específico de programa malintencionado que restringe el acceso mediante cifrado o determinadas partes o archivos del sistema infectado y pide un rescate (Generalmente en moneda virtual) a cambio de eliminar dicha restricción.

1.2. Objetivo

SERFOR	Evento: Ataque Informático – (E12)	OTI

Restaurar los servicios críticos de TI que soportan las estaciones de trabajo y servidores del Centro de Datos.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se puede producir durante el servicio, o en horario no laborable en el Centro de Datos del SERFOR.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialistas de Desarrollo y Aplicaciones
- Especialista de Base de Datos
- Especialista de redes y comunicaciones o quien haga sus veces
- Especialista de Soporte Técnico de OTI o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Contar con equipos de respuesta ante incidentes de seguridad ante posibles ataques informáticos en estaciones de trabajo y servidores.
- Contar con las copias de respaldo y cintas de backup probadas y actualizadas.
- Contar con antivirus actualizado en las estaciones de trabajo y servidores.
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Infección de virus informáticos en las estaciones de trabajo o servidores del centro de datos.

2.2. Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones del SERFOR.

2.3. Personal que autoriza la Contingencia

- Jefa o Jefe de la Oficina de Tecnologías de la Información del SERFOR.

2.4. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialistas de Desarrollo y Aplicaciones
- Especialista de Base de Datos
- Especialista de redes y comunicaciones o quien haga sus veces

SERFOR	Evento: Ataque Informático – (E12)	OTI

- Especialista de Soporte Técnico de OTI o quien haga sus veces.

2.5. Descripción de los procedimientos después de activar la contingencia:

- Detección del evento de infección de virus informático.
- Validar si trata de un ataque tipo RANSOMWARE
- Notificar al Jefe de OTI y equipo de respuesta de Incidentes de Seguridad.
- Establecer las medidas de contención para evitar su propagación a nivel toda la red.
- Validar si se puede apagar el equipo informático afectado, si es posible se procede a desconectar de la red al equipo informático.
- Si no es posible apagarlo, se verifica que no allá más equipos afectados.
- Se realiza un análisis inmediato considerando los siguientes criterios:
  - Riesgos e impactos en toda la red.
  - Clonación de discos
  - Deshabilitar servicios o sistemas
  - Ajustar reglas del Firewall y equipos de seguridad perimetral
  - Actualización de Antivirus.
- Proceder con las acciones de mitigación, considerando si equipo afectado está cifrado y posible su recuperación (Descifrable)
- Si no es posible proceder con la restauración de la copia de seguridad disponible.
- Si no es posible la restauración, se procede a formatear el equipo informático afectado.
- Restablecer las estaciones de trabo o servidores recuperados.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialistas de Desarrollo y Aplicaciones
- Especialista de Base de Datos
- Especialista de redes y comunicaciones o quien haga sus veces
- Especialista de Soporte Técnico de OTI o quien haga sus veces.

3.2. Descripción de actividades

- El especialista de administración de Data Center revisara que los servidores afectados se han restaurado y funcione con normalidad.
- El especialista de Soporte Técnico de OTI revisara que las estaciones de trabajo afectadas se han restaurado y funcione con normalidad
- El proveedor del Software Antivirus una vez solucionado el incidente emitirá un informe a la Jefatura de Tecnologías de la Información, detallando la causa origen del evento y las acciones realizadas.

SERFOR	Evento: Ataque Informático – (E12)	OTI

- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Información sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación
La OTI deberá asegurarse que las pruebas y revisiones periódicas a los servidores del Centro de Datos y estaciones de trabajo se lleven a cabo semestralmente.

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización
En base al informe presentado por el proveedor del sistema seguridad antivirus se tomarán las acciones correctivas y lecciones aprendidas para la actualización del Plan de Contingencia.

3.6. Tiempo de recuperación
El tiempo máximo de duración de la contingencia dependerá de la cantidad de equipos afectados, sin embargo, a nivel de tiempo por equipo informático se estima un máximo de 24 horas.

X. CRONOGRAMA DEL PLAN DE PRUEBAS

10.1. **Plan de Pruebas:** El Plan de Contingencias de TI comprende, el desarrollo de un plan de pruebas en el cual se incluye diferentes escenarios (Priorizados según plan) para comprobar que el plan diseñado es eficaz o, en caso contrario, se le debe efectuar ajustes correspondientes.

Los siguientes son los objetivos de control de las pruebas del plan:

a. Validar la habilidad de los responsables y la consistencia de los procedimientos en eventos de recuperación de siniestros.
b. Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados
c. Identificar y corregir falla en el Plan de Contingencias de TI
d. Facilitar la divulgación y el entrenamiento en los procedimientos de recuperación.
e. Fomentar el respeto por el plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias.
f. Motivar a los encargados involucrados en el diseño y desarrollo del Plan a mantener actualizados los procedimientos inherentes.

10.2. Cronograma de Pruebas

N°	EVENTO	2021					2022					
		Jun	Sept	Oct	Nov	Dic	Mar	May	Jun	Sep	Oct	Dic
E1	Caída o interrupción de energía eléctrica	X										
E2	Caída de internet										X	
E3	Infección masiva por software malicioso					X						
E4	Suspensión de las actividades por sismo o incendio											X
E6	Falla técnica en servidores		X									
E7	Falla en Sistemas de Información críticos								X			
E8	Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información, servidores y redes							X				
E9	Calentamiento del Centro de Datos						X					
E10	Falla técnica en equipos de comunicación				X							
E11	Falla técnica en equipos de clientes clave			X								
E12	Ataque informático									X		

Nota: El escenario 5 (E5) no se ha considerado porque solo se van a tratar los eventos de riesgos Muy Altas y Alta para el presente Plan de Contingencia de Tecnología de Información del SERFOR.

XI. PRESUPUESTO PARA LA EJECUCIÓN DEL PLAN DE CONTINGENCIA DE TI

El Plan de Contingencia de Tecnologías de la Información, contiene actividades que serán desarrolladas por el personal de la Oficina de Tecnologías de la Información de acuerdo con sus competencias; dichas actividades planificadas están contempladas en el presupuesto asignado a la OTI en el presente año y en los subsiguientes años fiscales.

XII. SEGUIMIENTO Y MEJORA CONTINUA

12.1. El responsable del mantenimiento y mejora continua del plan es el Oficial de Seguridad de la Información. El plan debe ser revisado, probado y actualizado en su documentación

y su alcance, esto quiere decir que el plan debe mejorado permanentemente a través de revisiones de acuerdo con los siguientes parámetros:

- Implementación de nuevos servicios críticos de TI: En caso se realicen nuevos Sistemas o servicios que soporten procesos críticos de la Institución se deberá realizar un mantenimiento de Plan de Contingencia.
- Resultados de una nueva evaluación de riesgos: Si dentro de la evaluación de riegos se identificación nuevos escenarios de criticidad Muy Alta o alta se deberán desarrollo o actualizar los procedimientos de recuperación.
- Requisitos legales o contractuales: Ante nuevas regulaciones establecidos por la administración pública a través de los TUPAs o normativas específicas.