Resolución del Secretario General No. 015-2021-TR/SG

Lima, 31 de marzo de 2021

VISTOS: El Informe N° 0019-2021-MTPE/4/13.2 de la Oficina de Tecnologías de la Información y Comunicaciones; el Memorando N° 1149-2020-MTPE/4/9 de la Oficina General de Planeamiento y Presupuesto; el Memorando N° 00536 -2020-MTPE/4.2 de la Oficina de Seguridad y Defensa Nacional; y el Informe Nº 0239-2021-MTPE/4/8 de la Oficina General de Asesoría Jurídica; y,

CONSIDERANDO:

Que, de acuerdo con el artículo 5 de la Ley N° 29381, Ley de Organización y Funciones del Ministerio de Trabajo y Promoción del Empleo, dicho Ministerio es el organismo rector en materia de trabajo y promoción del empleo;

Que, en las Normas de Control Interno, aprobadas por Resolución de Contraloría General Nº 320-2006-CG, se señala que para un adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio; y que para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia;

Que, la 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, establece que las entidades públicas integrantes del Sistema Nacional de Gestión del Riesgo de Desastres implementan la Gestión de la Continuidad Operativa, adecuándola a su alcance y a la complejidad de sus operaciones y servicios, bajo responsabilidad de la máxima autoridad de las mismas;

Que, en cumplimiento de lo dispuesto en la norma señalada en el considerando precedente, con Resolución Ministerial N° 250-2017-TR, el Ministerio de Trabajo y Promoción del Empleo aprueba su Plan de Continuidad Operativa, a fin de proporcionar la referencia de la información necesaria para recuperar, a nivel aceptable, los procesos/servicios de mayor criticidad de dicho Ministerio, ante la interrupción provocada por un evento disruptivo. Cabe señalar que el citado Plan está constituido, entre otros documentos de gestión, por el Plan de Contingencia Informático, al que define como el conjunto de procedimientos para garantizar la recuperación de los servicios de Tecnologías de la Información y restaurar las aplicaciones críticas o sistemas de soporte general;

Que, por otro lado, la Resolución Ministerial Nº 04-2016-PCM aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la

Información. Requisitos. 2a Edición", en todas las entidades del Sistema Nacional de Informática, la cual especifica los requisitos para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información de la institución; y establece un plazo de dos (02) años para que todas las entidades integrantes del Sistema Nacional de Informática se adecuen a dicha norma;

Que, asimismo, mediante Resolución Ministerial N° 213-2019-TR, el Ministerio de Trabajo y Promoción del Empleo aprueba la Política de Seguridad de la Información, con el objetivo de optimizar los controles de seguridad de la información en concordancia con los requisitos de dicho Ministerio y con las normas relacionadas al tratamiento de la información;

Que, mediante Resolución Ministerial N° 120-2014-TR, se aprueba el Plan de Contingencia Informático - PCI del Pliego 012: Ministerio de Trabajo y Promoción del Empleo;

Que, mediante el documento de vistos, la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones propone la aprobación de un nuevo Plan de Contingencia Informático para el MTPE, el mismo que ha sido elaborado por la Oficina de Tecnologías de la Información y Comunicaciones;

Que, respecto a la mencionada propuesta, la Oficina General de Planeamiento y Presupuesto y la Oficina de Seguridad y Defensa Nacional del MTPE han brindado opinión técnica favorable, a través del Memorando N° 1149-2020-MTPE/4/9 y del Memorando N° 00536 -2020-MTPE/4.2 respectivamente;

Que, en ese sentido, resulta necesario expedir el acto de administración interna que apruebe el Plan de Contingencia Informático del Ministerio de Trabajo y Promoción del Empleo;

Que, de acuerdo al literal c) del numeral 2.1 del artículo 2 de la Resolución Ministerial N° 006-2021-TR, que delega facultades y atribuciones en diversos funcionarios del Ministerio de Trabajo y Promoción del Empleo, durante el Año Fiscal 2021, el Titular de la Entidad delega al/a la Secretario/a General del Ministerio de Trabajo y Promoción del Empleo la facultad, entre otras, de aprobar, modificar, derogar, reordenar, todo documento de carácter normativo que regule actos de administración interna, así como otros documentos de gestión susceptibles de delegación, trámites internos, lineamientos técnico normativos y metodológicos, orientados a optimizar los procedimientos y procesos administrativos de carácter interno, a cargo de los órganos de apoyo y asesoramiento del Ministerio de Trabajo y Promoción del Empleo; así como dejar sin efecto toda normativa interna o documento de gestión que se le oponga;

REPÚBLICA DEL PERÚ

Resolución del Secretario General No. 015-2021-TR/SG

Con las visaciones de la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones, de la Oficina General de Planeamiento y Presupuesto, de la Oficina de Seguridad y Defensa Nacional, y de la Oficina General de Asesoría Jurídica; y,

De conformidad con la Ley N° 29381, Ley de Organización y Funciones del Ministerio de Trabajo y Promoción del Empleo; el Texto Integrado del Reglamento de Organización y Funciones del Ministerio de Trabajo y Promoción del Empleo, aprobado por la Resolución Ministerial N° 308-2019-TR; y, el literal c) del numeral 2.1 del artículo 2 de la Resolución Ministerial N° 006-2021-TR, que delega facultades y atribuciones en diversos funcionarios del Ministerio de Trabajo y Promoción del Empleo, durante el Año Fiscal 2021;

SE RESUELVE:

Artículo 1. Aprobar el Plan de Contingencia Informático del Ministerio de Trabajo y Promoción del Empleo, que como Anexo adjunto forma parte integrante de la presente Resolución.

Artículo 2. Derogar la Resolución Ministerial Nº 120-2014-TR, que aprueba el Plan de Contingencia Informático - PCI del Pliego 012: Ministerio de Trabajo y Promoción del Empleo.

Artículo 3. Disponer la publicación de la presente Resolución y de su Anexo aprobados en el artículo 1, en el Portal Institucional del Ministerio de Trabajo y Promoción del Empleo (www.gob.pe/mtpe), siendo responsable de dicha acción la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones.

Regístrese y comuníquese.

CARMEN MARIA MARROU GARCIA
Secretaria General
Ministerio de Trabajo y Promoción del Empleo

PERÚ Ministerio de Trabajo y Promoción del Empleo

MINISTERIO DE TRABAJO Y PROMOCIÓN DEL EMPLEO

OFICINA GENERAL DE ESTADÍSTICA Y TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

FIRMA DIGITAL
Firmado digitalmente por: HONORES CORONADO Jaime Alejandro FAU 20131023414 hard
Motivo: Doy V° B°
Fecha: 05/01/2021 17:27:18-0500

PLAN DE CONTINGENCIA INFORMÁTICO MINISTERIO DE TRABAJO Y PROMOCION DEL EMPLEO

Noviembre 2020

FIRMA DIGITAL
Firmado digitalmente por: GIBAJA ALVAREZ Daniel Alberto FAU 20131023414 soft
Motivo: Doy V° B°
Fecha: 25/11/2020 00:47:03-0500

FIRMA DIGITAL
Firmado digitalmente por: FIGUEROA HERNANDEZ Julio Gerardo FAU 20131023414 soft
Motivo: Doy V° B°
Fecha: 25/11/2020 11:35:44-0500

FIRMA DIGITAL
Firmado digitalmente por: TARMEÑO CHAVARRIA Johnny Albino FAU 20131023414 soft
Motivo: Doy V° B°
Fecha: 24/11/2020 22:10:31-0500

V° B° JEFATURA OGETIC

V 3.0

HISTORIAL DE CAMBIOS

Control de Configuración

Título:	Plan de Contingencia Informático del MTPE.
Autor:	Ing. Johnny Albino Tarmeño Chavarria
Fecha:	24 de noviembre de 2020

Histórico de Versiones

Versión	Fecha	Estado	Responsable	Descripción del Cambio
2.0	4 de setiembre de 2017	Elaborado/ Actualizado	Alejandro Arbildo Grández	Actualización del Plan de Contingencia Informático de la Oficina de Tecnologías de la Información y Comunicaciones V1.0
3.0	24 de noviembre de 2020	Elaborado/ Actualizado	Johnny Albino Tarmeño Chavarría	Actualización del Plan tomando en consideración los cambios en la plataforma tecnológica.

V° B° JEFATURA OGETIC

TABLA DE CONTENIDO

V° B° JEFATURA OGETIC

1. Presentación

El plan de contingencia informático de la UE001: Ministerio de Trabajo y Promoción del Empleo – Oficina General de Administración, tiene por finalidad establecer las pautas, la organización, las responsabilidades y desarrollar procedimientos que permitan asegurar una eficiente capacidad de las tecnologías de información y comunicaciones ante desastres y otras situaciones de emergencia, con el propósito de mantener la continuidad operativa de los servicios informáticos de la institución.

2. Diagnóstico general

La necesidad de actualizar el plan de contingencia informático de una v.2.0. a una v.3.0, se debe a que la plataforma tecnología ha cambiado desde el 29 de setiembre del 2017 hasta el presente. Por tal motivo, se deben redefinir los escenarios, actividades y recursos asociados a las nuevas condiciones.

Cabe destacar que el Plan de Contingencia Informático v.2.0. no fue ejecutado, ya que no se presentaron los escenarios de contingencia planteados en el mismo. Al no ser ejecutado, no se tuvieron resultados que fueran incluidos o considerados para el presente Plan.

3. Base legal

3.1. Resolución Ministerial Nº 258-2016-TR, que constituye el Comité de Gestión de Seguridad de la Información del MTPE.

3.2. Resolución Ministerial N° 111-2019-TR, que aprueba la ampliación de metas del Plan Estratégico Sectorial Multianual (PESEM) 2017–2021 del Sector Trabajo y Promoción del Empleo y el Plan Estratégico Institucional (PEI) 2017-2021 del Ministerio de Trabajo y Promoción del Empleo (MTPE) al año 2022 (MTPE).

3.3. Resolución Ministerial Nº 115-2019-TR, que modifica la R. M. Nº 236-2018-TR, que constituyó el Comité de Gobierno Digital del MTPE.

3.4. Resolución Ministerial Nº 001-2020-TR, que aprueba el Plan Operativo Institucional (POI) 2020 del Ministerio de Trabajo y Promoción del Empleo (MTPE)

3.5. Reglamento de Organización y Funciones 2017, que define la funciones de la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones. Artículo 42. Ítem c y g.

3.6. Resolución Ministerial Nº 04-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

V° B° JEFATURA OGETIC

3.7. Resolución Ministerial N° 028-2015-PCM Resolución que aprueba los lineamientos para la gestión de la continuidad operativa de las entidades públicas en los tres niveles de gobierno.

3.8. Resolución de Contraloría General N° 320-2006-CG, Normas de Control Interno.

4. Finalidad

El plan de contingencia informático tiene por finalidad servir de hoja de ruta de acción, ante la materialización de escenarios críticos contingentes previamente definidos, que afecten la continuidad de la disponibilidad de las operaciones, el procesamiento de datos y aplicaciones vitales, ante los escenarios de desastres determinados, definiendo las acciones a realizar de manera previa, durante y después de la materialización de un riesgo que los afecte.

5. Objetivos

5.1. Objetivo Estratégico Sectorial e Institucional con el cual se vincula

Los Objetivos del presente Plan están alineados al objetivo estratégico sectorial OE6 "Implementar un efectivo modelo de gestión sectorial centro en el ciudadano" y al objetivo estratégico institucional OEI8 "Mejorar el modelo de gestión institucional centrado en el ciudadano", Acción estratégica AEI.8.2 "Sistemas Administrativos modernizados con herramientas de gestión orientadas al beneficio de clientes interno y externos".

5.2. Objetivo general

Establecer procedimientos y acciones a realizar ante eventos de materialización de riesgos que afecten la infraestructura tecnológica critica institucional, situación que podría alterar y/o paralizar los procesos operativos de la institución, buscando la recuperación de los servicios informáticos en forma rápida, eficiente y oportuna.

5.3. Objetivos específicos

- Definir la organización de la contingencia y los roles de los actores.
- Definir el proceso de activación del Plan de Contingencia Informático.
- Desarrollar los procedimientos de contingencia para recuperar la operatividad de los sistemas informáticos de la institución.

V° B° JEFATURA OGETIC

6. Estrategias

La estrategia para el logro de los objetivos del presente plan consistirá en que la determinación de los escenarios de contingencia responda a los riesgos residuales de la Matriz de Riesgos – Nivel Procesos de la OGETIC y a su impacto, cuya causa raíz esté asociada a la indisponibilidad de la Plataforma Tecnológica e impacte a las áreas de negocio.

6.1. Riesgos de los procesos a cargo de la OGETIC

A continuación, se muestran los Riesgos – Nivel Procesos de la OGETIC y, cuya causa raíz está asociada a la indisponibilidad de la Plataforma Tecnológica e impacte a las áreas de negocio.

Cabe recordar que se están considerando solo los riesgos de proceso de OGETIC, sin embargo, se podrán agregar los riesgos a nivel entidad que se identifiquen a futuro.

Riesgo	Tipo de Riesgo	Causa	Consecuencia	Nivel de riesgo residual	Acción a Realizar
Posibilidad de caída del servidor que contiene la Data de la Planilla Electrónica.	Tecnológico	Caída del servidor	No poder entregar Información oportunamente a la Alta Dirección	4 Moderado	**Reducir**
Caída de servidores que contienen información importante del MTPE (planillas electrónicas), conllevaría a no poder entregar información oportunamente a la Alta Dirección	Tecnológico	Falta de tecnología / Caída del servidor	Se detienen los Procesos Core del negocio de la institución el cual puede conllevar a incumplimiento de temas legales, afecta la imagen de la entidad.	4 Moderado	**Reducir**

6.2. Descripción de los escenarios de Contingencia

Los escenarios de contingencia asociados a los riesgos del numeral 6.1, mismos en que se podría dar la "Caída de un Servidor" o la "Indisponibilidad de Equipos Servidores", a pesar de que se hayan implementado controles, se relacionan con situaciones externas a la OTIC, las cuales se indican a continuación

- Escenario 1 - Pérdida de suministro eléctrico. De haber un corte del fluido eléctrico de nuestro proveedor de servicios, el MTPE ha implementado grupos electrógenos que nos permiten seguir operando y no afectar el funcionamiento

del centro de Datos. Se tomará esté escenario considerando actividades contingentes cuando también se vea afectado el funcionamiento del grupo electrógeno.

- Escenario 2 - Infección de un equipo por malware. Ante la aparición de software malicioso en la red (malware), el MTPE ha implementado software de protección de equipos de escritorio para eliminar, virus, malware, adware y otros tipos de software maliciosos; lo que permite a los equipos seguir operando y no afectar a los usuarios que quieran hacer uso de los servicios brindados por nuestra plataforma tecnológica. Se tomará esté escenario considerando actividades contingentes cuando a pesar de los controles implementados, se vea afectado un equipo de cómputo.

- Escenario 3 - No disponibilidad de un sistema de información. Ante debilidades de software o hardware que provoquen la indisponibilidad de un sistema de información, el MTPE ha implementado sistemas de redundancia y balanceo de carga; lo que permite que el servicio siga operando y no afectar a los usuarios que quieran hacer uso de los servicios brindados por nuestra plataforma tecnológica. Se tomará esté escenario considerando actividades contingentes cuando a pesar de los controles implementados, se vea afectado un sistema de información.

6.3. Formato estándar de los escenarios de contingencia asociados a las causas de los riesgos

La estrategia usada para definir los escenarios, consiste en detallar las actividades de contingencia, los responsables de ejecutarlas y los recursos que deben estar disponibles para su correcta ejecución. Esta información se redacta en forma de procedimiento o guía práctica, el cual debe ser de claro entendimiento por el personal de la institución.

Se considerará un formato estándar de registro de los escenarios que forman parte del plan. Cada procedimiento de contingencia contendrá como mínimo la siguiente información:

N°	Componentes	Descripción
1	Procedimiento.	Código y Nombre del Procedimiento de Contingencia.
2	Objetivo	Fin que persigue el procedimiento.
3	Evento y Riesgo	Detalle del evento. Referencia a la amenaza y riesgo, previamente analizado.
4	Roles	Roles intervinientes en las actividades.

V° B° JEFATURA OGETIC

N°	Componentes	Descripción
5	Fase previa	Acciones que se realizan o aseguran de manera permanente en la institución, y que permiten que se ejecuten las acciones contingentes.
6	Fase de ejecución	Acciones a realizar en el momento que ocurre el evento de contingencia.
7	Fase de recuperación	Acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones que fueron afectadas por un evento de contingencia.

7. Órganos y Unidades Orgánicas responsables

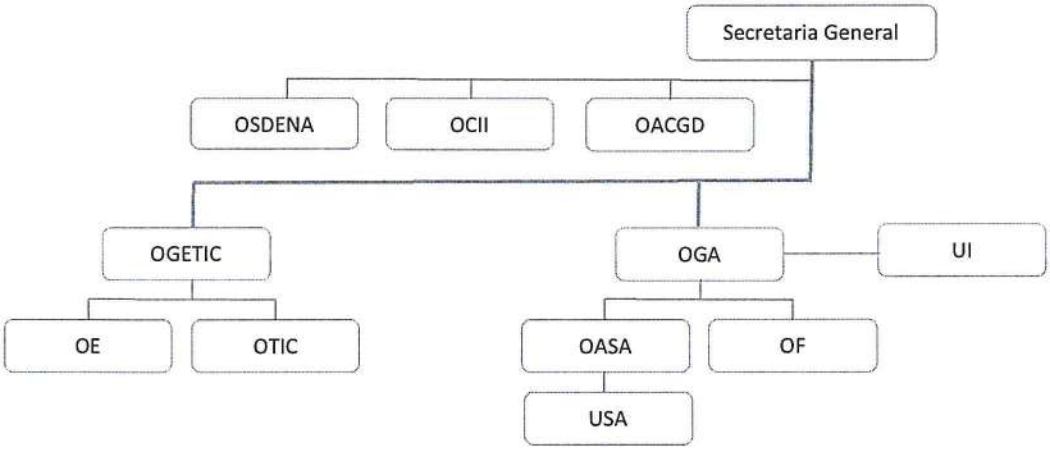

Figura 1. Órganos y Unidades Orgánicas responsables

Donde:
OSDENA: Oficina de Seguridad y Defensa Nacional
OCII: Oficina de Comunicación e Imagen Institucional
OACGD: Oficina de Atención al Ciudadano y Gestión Documentaria
OGA: Oficina general de Administración
UI: Unidad de Infraestructura
OF: Oficina de Finanzas
OASA: Oficina de Abastecimiento y Servicios Auxiliares
USA: Unidad de Servicios Auxiliares
OGETIC: Oficina General de Estadística y Tecnologías de la Información y Comunicaciones.
OTIC: Oficina de Tecnologías de la Información y Comunicaciones.
OE: Oficina de Estadística

V° B° JEFATURA OGETIC

7.1. Gestores de la Contingencia Tecnológica

- Jefe de la Oficina de Tecnologías de la Información y Comunicaciones (OTIC). Función: Mantener actualizado el Plan de Contingencia Informático.
- Jefe de la Unidad de Servicios Auxiliares (USA – OASA).
- Jefe de la Unidad de Infraestructura (UI – OGA).
- Jefe de la Oficina de Seguridad y Defensa Nacional (OSDENA).

Funciones generales:

- Proponer modificaciones y/o correcciones al presente plan.
- Asegurar que el personal involucrado se encuentre capacitado, según las acciones que deba realizar asociadas al presente plan.
- Asegurar el suministro de recursos necesarios para asegurar la viabilidad del presente plan.

7.2. Autorizadores:

- Su función es autorizar el inicio de las acciones de contingencia.
- En caso de no encontrarse, podrá asignar a otro personal alterno a dicho rol.
- Los cargos asociados se indicarán en cada procedimiento del presente Plan de Contingencia.

7.3. Ejecutores:

- Su función es realizar las actividades operativas preventivas, correctivas y de recuperación para poner en marcha el proceso de cada escenario de contingencia respectivo.
- En caso de no encontrarse, podrá asignar a otro personal alterno a dicho rol.
- Los cargos asociados se indicarán en cada procedimiento del presente Plan de Contingencia.

8. Ámbito de Intervención

El Plan de Contingencia informático tiene un alcance institucional e involucra sólo a la Unidad Ejecutora 001. Este Plan abarca los aspectos que forman parte del servicio informático y de su infraestructura tecnológica y está alineado la Matriz de Riesgo OTIC – Nivel Entidad. En tal sentido, se considerarán los riesgos residuales que requieren la planificación de acciones contingentes.

Los principales elementos que están en el alcance de la contingencia son:

Tipo de Recursos	Descripción y comentarios
1. Recursos de Hardware y Software	**Plataforma de Procesamiento y Almacenamiento** o Servidores o Repositorios o Firewalls o UPS

V° B° JEFATURA OGETIC

Tipo de Recursos	Descripción y comentarios
	○ Librerías de copias de respaldo **Plataforma Lógica** ○ Web Services externos a SUNAT, Banco de la Nación, RENIEC ○ Sistemas Operativos ○ Sistemas Informáticos ○ Sistemas Ofimáticos y Especializados ○ Software de Bases de Datos **Plataforma de Comunicaciones** ○ Switches ○ Redes inalámbricas ○ Cableado de Red (Fibra y Cobre) ○ Líneas Dedicadas ○ Servicio de Internet ○ UPS **Plataforma del Cliente** ○ Impresoras y equipos multifuncionales. ○ PC de usuario.
2. Recursos Públicos	**Servicios Públicos** ○ Suministro de energía eléctrica. ○ Suministro de agua.
3. Recursos presupuestales	Este plan no hará uso de recursos presupuestales adicionales a los ya aprobados en la meta presupuestaria de los órganos y unidades orgánicas responsables de la ejecución del plan, mismos que se indican en el numeral 7 del presente plan.

9. Beneficiarios

El plan de contingencia informático, en cuanto se ejecute, busca beneficiar a los ciudadanos que consumen servicios digitales de la institución, a los órganos y unidades orgánicas cuya labor y operaciones dependen de los servicios digitales internos y a la OGETIC en relación al oportuno cumplimiento de sus funciones.

10. Implementación

Procedimientos de contingencia que responderán a la ocurrencia de los escenarios definidos en el punto:

- Escenario 1 - Pérdida de suministro eléctrico.
- Escenario 2 - Infección de un equipo por malware.
- Escenario 3 - No disponibilidad de un sistema de información.

V° B° JEFATURA OGETIC

10.1. Procedimiento: PRO-CON-01/V2 - Procedimiento de Contingencia en caso de pérdida del suministro eléctrico

Objetivo
Restaurar las funciones consideradas como críticas para el centro de datos.
Evento y Riesgo
Interrupción del suministro eléctrico: Corte de suministro de energía eléctrica en los ambientes del Centro de Datos de la Sede Central de la institución. **Activador:** Detección del corte del suministro eléctrico, por cualquier personal de la institución. Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia: Servicios públicos • Suministro de energía eléctrica. • Servicio de interconexión entre sedes. • Servicio de internet. • Servicios informáticos de uso del ciudadano y empresas. • Servicio de Central Telefónica. Hardware • Servidores • Firewalls • Librería de copia de respaldo • Estaciones de trabajo • Equipos de comunicaciones en red. Equipos diversos • Sistema de climatización (Aire acondicionado de precisión) • UPS • Grupo Electrógeno
Roles
Autorizadores: • No se requiere autorización para el inicio de la contingencia ya que inicia con un proceso automático. • Se requiere una autorización para el apagado de la Infraestructura Tecnológica. Los autorizadores serán el Jefe de la OGETIC y en su defecto el Jefe de la OTIC. Ejecutores • Administrador de Red – OTIC. • Administrador de Servidores - OTIC. • Administrador de Base de Datos – OTIC. • Coordinador de Soporte Técnico – OTIC. • Coordinador de Infraestructura Tecnológica – OTIC. • Coordinadores de Desarrollo – OTIC. • Oficial de Seguridad de la Información. • Personal del Taller de Electricidad y Sonido USA-OASA. • Personal de OSDENA. • Jefe de la OTIC. • Jefe de la UI.

V° B° JEFATURA OGETIC

- Jefe de la OASA.
- Jefe de OSDENA.

Apoyo
- Personal del Taller de Electricidad y Sonido USA-OASA.
- Especialista en Electricidad de la UI-OGA.

Fase Previa

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	Asegurar que el equipo (o los equipos) UPS del Centro de Datos cuente con el mantenimiento respectivo.	Servicio de Mantenimiento Preventivo por Terceros	Administrador de Red - OTIC	Anualmente y por evento
2	Realizar pruebas periódicas del UPS (con apoyo del Personal del Taller de Electricidad y Sonido USA-OASA).	Documento Protocolo de Pruebas	Administrador de Red –OTIC	Anualmente
3	Realizar mantenimiento preventivo del grupo electrógeno.	Servicio por terceros	Personal del Taller de Electricidad y Sonido USA-OASA	Cada 6 meses
4	Ejecutar protocolos de prueba de arranque en vacío del grupo electrógeno (con apoyo del Especialista en Electricidad de la UI-OGA).		Personal del Taller de Electricidad y Sonido USA-OASA	Cada 7 días
5	Ejecutar mantenimiento preventivo de los sistemas de pozo a tierra.	Servicios por terceros	Personal del Taller de Electricidad y Sonido USA-OASA	Cada 6 meses
6	Realizar limpieza física periódica de todos los gabinetes de comunicaciones y los equipos incluidos.	Artículos de limpieza, Llaves de Gabinetes	Administrador de Red - OTIC	Cada 6 meses
7	Verificar se cuente con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso. En alineación al Plan de Continuidad de Negocio aprobado y vigente.	Plan de Continuidad de Negocio MTPE	Se encarga cada área operativa.	Anualmente
8	Verificación de los sistemas informáticos en la máquina virtual de contingencia operativa para usuario final,	Una máquina virtual preparada Una consola KVM	Administrador de Servidores - OTIC	2 meses

V° B° JEFATURA OGETIC

N°	Actividad	Recursos	Ejecutor	Tiempo
	preparada y habilitada en el Centro de Datos.			
9	Consultar periódicamente a la empresa proveedora del servicio de suministro eléctrico para conocer si se programarán cortes de fluido eléctrico y el tiempo de duración de estos, para tomar las previsiones del caso.		Personal del Taller de Electricidad y Sonido USA-OASA	Permanente

Fase de Ejecución

(a) En Horario Laboral

(b) Fuera de Horario Laboral

N°	Actividad	Recursos	Ejecutor	Tiempo
1	Activación Automática del Grupo Electrógeno.	Grupo electrógeno	Sistema Automático	15 segundos
2	Informar al jefe de la OTIC y al Administrador de Red respecto al corte de fluido eléctrico, de manera imprevista (por correo electrónico y/o por equipo celular).		(a) Personal del Taller de Electricidad y Sonido USA-OASA (b) Personal de OSDENA	02 minutos
3	Verificar que, ante la pérdida del servicio de suministro eléctrico, el grupo electrógeno comience a operar automáticamente a través del tablero de transferencia automático. Si no levanta el grupo electrógeno. Ir al Punto 9.		(a) Personal del Taller de Electricidad y Sonido USA-OASA (b) Personal de OSDENA	05 minutos
4	Si hay retorno del suministro de energía eléctrica comercial, apagar el grupo electrógeno y verificar el funcionamiento del UPS y del tablero de transferencia automático.		(a) Personal del Taller de Electricidad y Sonido USA-OASA (b) Personal de OSDENA	05 minutos
5	Informar al jefe de la OTIC y al Administrador de Redes de la Información sobre el retorno del suministro eléctrico.		(a) Personal del Taller de Electricidad y Sonido USA-OASA (b) Personal de OSDENA	02 minutos
6	Registrar el incidente.		Administrador de Red - OTIC	02 minutos

V° B° JEFATURA OSETIC

N°	Actividad	Recursos	Ejecutor	Tiempo
7	Comunicar a las partes interesadas respecto a la recuperación del servicio (Por correo, mensajes SMS, u otros).	Listado de Partes interesadas	Coordinador de Soporte Técnico - OTIC	02 minutos
8	El Jefe de la OTIC deberá comunicar al Jefe de la OGETIC respecto a las acciones realizadas y el estado de los servicios.		Jefe de OTIC	05 minutos
9	Si no retorna el suministro de energía eléctrica comercial, verificar la reserva de combustible. ➢ Si la reserva de combustible está a menos de la mitad del tanque solicitar el abastecimiento de combustible. ➢ Si no existe abastecimiento oportuno y el grupo electrógeno se apaga comunicar al jefe de la OGETIC (Jefe de OTIC en su defecto) para que autoricen el apagado de los servidores. Ir a la Fase de Recuperación		Personal del Taller de Electricidad y Sonido USA-OASA.	Cada 02 horas
Consideraciones: • El tiempo máximo de duración de la contingencia dependerá del soporte en el tiempo que provea el Grupo Electrógeno. • El retorno del suministro eléctrico dependerá del proveedor externo del servicio de suministro eléctrico.				

Fase de Recuperación

N°	Actividad	Recursos	Ejecutor	Tiempo
1	Comprobar el restablecimiento del fluido eléctrico (con apoyo del Especialista en Electricidad de UI-OGA)		Personal del Taller de Electricidad y Sonido USA-OASA	05 minutos
2	De haber sido necesario el apagado de los servidores: habilitar la plataforma tecnológica.	Protocolo de Prueba	Coordinador de Infraestructura Tecnológica - OTIC	4 horas
3	Monitorear los servicios de base de datos.	Herramienta de Monitoreo	Administrador de Base de Datos - OTIC	1 hora

V°B° JEFATURA OGETIC

Nº	Actividad	Recursos	Ejecutor	Tiempo
4	Monitorear los servidores de las aplicaciones	Herramienta de Monitoreo	Administrador de Servidores – OTIC Coordinadores de Desarrollo-OTIC	1 hora
5	Verificar el correcto funcionamiento del sistema de aire acondicionado de precisión; así como verificar los valores que marcan los indicadores de temperatura de los gabinetes del Centro de Datos.	Protocolo de Prueba	Administrador de Red – OTIC	1 hora
6	Desactivar el Plan de Contingencia una vez comprobado la funcionalidad de los servicios informáticos del Centro de Datos.	Plan de Contingencia Informático	Jefe de la OTIC	
7	Evaluar las actividades del evento, y de ser necesario, registrar la misma en el formato de ocurrencia de eventos. (Evaluación de cumplimiento de actividades, tiempos y eficacia).		Administrador de Red - OTIC / Oficial de Seguridad de Información	01 hora
8	Presentar el Reporte del Incidente al jefe de la OTIC, indicando que parte del servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.		Oficial de Seguridad de Información	2 días
9	Gestionar las medidas preventivas y correctivas del caso.		Jefe de OTIC, Jefe de USA Jefe de UI Jefe de OSDENA	1 semana
10	Actualizar el Plan de Contingencia de acuerdo a las mejoras detectadas para implementación	Plan de Contingencia Informático	Coordinador de Infraestructura Tecnológica - OTIC	01 día

V° B° JEFATURA OGETIC

10.2. PRO-CON-02/V2: Procedimiento de Contingencia en caso de infección de un equipo por malware.

Objetivo
Evitar la pérdida de información institucional
Evento y Riesgo
Infección de un equipo por malware. **Activador**: • Reporte de un usuario que advierte mensajes de malware o ransomware en su equipo de cómputo. • Mensajes de error durante la ejecución de programas • Lentitud en el acceso a las aplicaciones • Falla general en el equipo (sistema operativo, aplicaciones) • Anuncios de ataques por los grupos de activistas como Anonymous. Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia: Servicios públicos • Servicio de interconexión entre sedes. • Servicio de internet. • Servicio de Redes Inalámbricas. Hardware • Servidores de archivo. • Estaciones de trabajo. • Equipos de comunicaciones en red. • Puntos de Acceso Inalámbricos Software • Servicio Antivirus y Antimalware • Software de Clonación de PC's Información: • Inventario de PC's
Roles
Autorizadores: • Jefe de la Oficina de Tecnologías de la Información y Comunicaciones – OTIC. • Coordinador de Infraestructura Tecnológica – OTIC • Coordinador de Soporte técnico - OTIC. • Oficial de Seguridad de la Información. Ejecutores • Coordinador de Infraestructura Tecnológica – OTIC • Coordinador de Soporte Técnico – OTIC. • Administrador de Red - OTIC. • Administrador de Servidores - OTIC. • Personal de Soporte Técnico.

V°B° JEFATURA OGETIC

Fase Previa

N°	Actividad	Recursos	Ejecutor	Tiempo
1	Verificar que todas las PC's se encuentren conectadas a la consola del antivirus y, que todas las funcionalidades del antivirus en dichas PC's, estén activas.	Consola de Antivirus	Coordinador de Infraestructura Tecnológica	2 veces a la semana
2	Verificar que la consola se actualice continuamente (Firewall, firmas).	Consola de Antivirus	Coordinador de Infraestructura Tecnológica	2 veces a la semana
3	Verificar que los equipos de seguridad perimetral (Firewall), se actualice en forma continua (solo firmas).	Firewall	Administrador de servidores	2 veces a la semana
4	Verificar que las alertas ante Bootnet y Callback estén habilitadas en los firewalls.	Firewall	Administrador de servidores	1 vez a la semana
5	Validación / Optimización de las reglas del firewall, evaluando y comunicando, a la Mesa de Ayuda, el impacto que podría tener para los usuarios.	Firewall	Administrador de servidores	1 vez al mes
6	Verificar en el Firewall a diario eventos de CALL BACK debido a que estos indican las PC infectadas con malware.	Firewall	Administrador de servidores	Diariamente
7	Atender la presencia de Malware ante solicitud de Administrador de Red.		Personal de Soporte Técnico	A demanda
8	En el Firewall configurar bloqueo geográfico (solo en el caso de ataques programados o anunciados).	Firewall	Administrador de servidores	A demanda
9	Programar el antivirus para realizar un escaneo a todos los equipos de cómputo y servidores con una frecuencia semanal.	Consola de Antivirus	Administrador de Red	1 vez a la semana
10	Inscribir en la lista negra de filtro de contenidos las direcciones IP y las URL de los CALLBACK.	Firewall	Administrador de servidores Administrador de Red	A demanda
11	Revisar periódicamente las políticas de antivirus, principalmente la de control de aplicaciones.	Consola Antivirus	Administrador de Red	1 vez a la semana
12	Restringir el acceso a Internet a los equipos de cómputo que por su uso no lo requieran, sobre PC's no	Firewall	Administrador de Red	1 vez al mes

V° B° JEFATURA OGETIC

Nº	Actividad	Recursos	Ejecutor	Tiempo
	usadas por personal en funciones.			
13	Implementación de políticas para el uso de quemadores de CD/DVD, entre otros, en estaciones de trabajo que no lo requieran.	Directorio Activo Consola de Antivirus	Administrador de Red Administrador de servidores	1 vez al mes
14	Deshabilitar los puertos de comunicación USB en los equipos de cómputo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.	Directorio Activo Consola de Antivirus	Administrador de Red Administrador de servidores	1 vez al mes
15	Actualizar parches de seguridad del sistema operativo y de los aplicativos en las PC de los usuarios.	Proceso Automático por WSUS	Administrador de servidores	Diariamente
16	Actualizar parches de seguridad del sistema operativo y de los aplicativos, en los servidores y en las bases de datos (Windows y Linux).		Administrador de servidores	1 vez al mes
17	Realizar servicio de Ethical Hacking desde fuera y dentro de la entidad.		Coordinador de Infraestructura Tecnológica	Semestral
18	Mantener el inventario PC's actualizado y compartido con infraestructura, código patrimonial.		Personal de Soporte Técnico	Permanente

Fase de Ejecución

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	Comunicar al Coordinador de Infraestructura Tecnológica la Activación del Plan de Contingencia.		Personal de Soporte Técnico	05 minutos
2	Retirar el equipo infectado de la red de datos interna. Lacrar los puertos de la PC y poner indicativo para evitar su uso. • Red física: desconectar • WiFi: Comunicar a Infraestructura tecnológica los 4 últimos dígitos el código patrimonial para desconectar).	Protocolo de desconexión de equipos en Redes Inalámbricas y en sedes remotas	Personal de Soporte Técnico	05 minutos

V° B° JEFATURA OGETIC

Nº	Actividad	Recursos	Ejecutor	Tiempo
3	Solicitar entrega de todos los dispositivos extraíbles que se hayan usado en la PC (hasta de dos días antes) y retener.		Personal de Soporte Técnico	10 minutos
4	Identificar destino y origen de tráfico malicioso de la PC comprometida.		Administrador de servidores	15 minutos
5	Identificar otras PC's o equipos que pudieran estar comprometidas.		Administrador de servidores	15 minutos
6	Retirar dichos equipos de la red (Wifi) y/o remitir listado a Soporte técnico para que sean retirados.		Administrador de servidores	30 minutos
7	Retirar equipos de la red. Lacrar los puertos de la PC y poner indicativo para evitar su uso. Solicitar entrega de todos los dispositivos extraíbles que se hayan usado en la PC (hasta de dos días antes) y retener.		Personal de Soporte Técnico	15 minutos por PC
8	Entregar nuevas PC's a los usuarios, según disponibilidad,		Personal de Soporte Técnico	4 horas
Consideraciones: Si los eventos ocurren en una sede remota, los tiempos asociados a las actividades del Personal de Soporte Técnico podrían aumentar en dos horas.				

Fase de Recuperación

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	Clonar información de los equipos comprometidos, de ser posible.		Personal de Soporte Técnico	1 hora por PC
2	Extraer información de los procesos y la muestra para enviarlos al proveedor del Servicio de Seguridad de EndPoint. Incluir información de los dispositivos extraíbles que se hayan usado en la PC y de todas las posibles PC's comprometidas.		Personal de Soporte Técnico Administrador de Red	1 hora
3	Investigar y coordinar con el proveedor del Servicio de Seguridad de EndPoint, y entregar a Mesa de Ayuda un procedimiento para eliminar el agente causante de la infección y remover el	Servicio de Antivirus y Antimalware	Administrador de Red	24 horas

V° B° JEFATURA OGETIC

Nº	Actividad	Recursos	Ejecutor	Tiempo
	malware de las PC's comprometidas.			
4	Ejecutar procedimiento de recuperación de las PC's comprometidas.		Personal de Soporte Técnico	1 hora por PC
5	Para la recuperación de información, entregar a Mesa de Ayuda un procedimiento para recuperar los datos. De no haberse encontrado una solución, ordenar el formateo de los equipos previa autorización del Área Usuaria		Administrador de Red	1 semana desde el registro del incidente
6a	Sí no se logró recuperar la información: • Asegurar que el equipo fue clonado. • Formatear equipo. • Restaurar con el software base para ponerlo a disposición nuevamente.		Personal de Soporte Técnico	1 hora por PC
6b	Si se logró recuperar la información: • Personalizar la estación para el usuario. • Conectar el equipo a la red de datos interna • Efectuar las pruebas necesarias con el equipo de cómputo.		Personal de Soporte Técnico	1 hora por PC
7	Luego de restaurar el correcto funcionamiento del equipo de cómputo, coordinar con el usuario responsable y/o jefe del área para reanudar las labores de trabajo con el equipo. En el caso el equipo infectado sea un servidor, el encargado será el administrador de dicho servidor.		Personal Soporte Técnico	10 minutos
8	Informar al Coordinador de Soporte Técnico el tipo de virus encontrado y el procedimiento usado para removerlo. En función a esto, se tomarán las medidas preventivas adicionales.		Coordinador de Infraestructura Tecnológica	1 hora

V° B° JEFATURA OGETIC

Nº	Actividad	Recursos	Ejecutor	Tiempo
9	Registrar cono ticket en Mesa de ayuda con la revisión del Oficial de Seguridad de Información o quien haga sus veces		Coordinador de Soporte Técnico	15 minutos
10	Con el aviso del personal de Soporte Técnico o del Administrador de los servidores, se desactivará el presente Plan.		Administrador de Servidores Personal de Soporte Técnico	5 minutos

10.3. PRO-CON-03/V2: Procedimiento de contingencia en caso de la no disponibilidad de un sistema de información

Objetivo
Mantener operativos los servidores de producción donde se ejecutan las aplicaciones institucionales.
Evento y Riesgo
Indisponibilidad de un Sistema de Información. **Activador**: • Falla de acceso a las aplicaciones. • Mensaje de pérdida de conexión a la base de datos. Es la ausencia de interacción entre el software y el hardware haciendo inoperativa la máquina; es decir, el software no envía instrucciones al hardware imposibilitando su funcionamiento. Este evento incluye los siguientes elementos mínimos, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestra a continuación: Software: • Software de sistemas operativos • Sistemas ofimáticos o especializados • Lenguajes de programación • Aplicativos y sistemas informáticos institucionales • Web Services externos a la institución. Hardware: • Servidores Información: • Copias de respaldo de base de datos • Copias de respaldo de las aplicaciones o sistemas informáticos utilizados • Copias de respaldo de software base (sistemas operativos y otros necesarios). Los servidores de aplicaciones están situados en el Centro de Datos, Piso 9, Oficina de Tecnologías de la Información y Comunicaciones, Sede Central.
Roles
Autorizadores: • Jefe de la Oficina General de Estadística, Tecnologías de la Información y Comunicaciones – OGETIC.

V° B° JEFATURA OGETIC

- Jefe de la Oficina de Tecnologías de la Información y Comunicaciones – OTIC.

Ejecutores

- Coordinador de Infraestructura Tecnológica – OTIC
- Coordinadores de Desarrollo – OTIC
- Coordinador de Soporte Técnico – OTIC.
- Administrador de Servidores - OTIC.
- Oficial de Seguridad de la Información.
- Jefe de la Oficina de Tecnologías de la Información y Comunicaciones – OTIC.

Fase de Previa

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	Contar con equipos de respaldo ante posibles faltas de los servidores.		Coordinador de Infraestructura Tecnológica	Permanente
2	Contar con mantenimiento preventivo para dichos equipos.		Coordinador de Infraestructura Tecnológica	Anualmente
3	Contar con copias de resguardo de la información, necesarias para restablecer las aplicaciones.		Administrador de Servidores	Permanente
4	Contar con copias de respaldo de las aplicaciones y de las bases de datos.		Administrador de Servidores	Permanente
5	Almacenar en un lugar seguir las copias de respaldo referidos a aplicaciones y datos.		Administrador de Servidores	Permanente
6	Custodia externa de una segunda copia de respaldo (fuera de la institución).		Administrador de Servidores	Permanente

Fase de Ejecución:

Caso 1: Servicio afectado basado en Máquinas Virtuales

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	Acceder a las copias de resguardo de los servidores virtuales.		Administrador de Servidores	15 minutos
2	De hallarse disponible la Solución de Virtualización instalada en el Centro de Datos, levantar el servidor virtual, previo chequeo de la capacidad de		Administrador de Servidores	30 minutos

V° B° JEFATURA OGETIC

	procesamiento y de almacenamiento de la solución de virtualización.			
3	Verificar la conectividad y funcionamiento de las interfaces entre el Servicio Publicado y otros servicios relacionados a este.		Administrador de Servidores Coordinadores de Desarrollo	2 horas

Fase de Ejecución:

Caso 2: Servicio afectado basado en Servicios Físico

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	Acceder a las copias de resguardo de las imágenes de los servidores, ISOs, o en su defecto del software de sistemas operativos, de servicio y de base de datos., según su software base y tecnología.		Administrador de Servidores	15 minutos
2	Implementar el servicio en el Servidor de Contingencia destinado para tal fin.		Administrador de Servidores	2 horas
3	Verificar la conectividad y funcionamiento de las interfaces entre el Servicio Publicado y otros servicios relacionados a este.		Administrador de Servidores Coordinadores de Desarrollo	2 horas

Fase de Ejecución: Generalidades

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	Se deberán reconfigurar los valores DNS e IPs relacionados al servicio.		Administrador de Servidores	15 minutos
2	Verificar que los servicios dependientes del servicio sobre el cual se ha activado la contingencia, están disponibles y funciones sin problemas.		Administrador de Servidores Coordinadores de Desarrollo	2 horas
3	Monitorear el desempeño de la nueva infraestructura usada como contingencia, hasta que sea desactivado el Plan de Contingencia.		Administrador de Servidores Coordinadores de Desarrollo	2 horas
4	Comunicar a los usuarios líderes del proceso relacionado al servicio afectado, que se ha activado el Plan de Contingencia respectivo.		Coordinador de Soporte Técnico	5 minutos

V° B° JEFATURA OGETIC

5	Registrar el formato de ocurrencia de eventos y se remitirá al Oficial de Seguridad de la Información (o quien haga las veces) para su revisión.		Oficial de Seguridad de Información	15 minutos
6	Con el aviso del Jefe de la Oficina de Tecnologías de la Información y Comunicaciones, desactivar el presente plan		Jefe OTIC	5 minutos

Consideraciones:

- Cabe mencionar, que el personal que opera los aplicativos y sistemas informáticos institucionales debe poner en práctica su proceso manual, mientras dure la contingencia.
- La duración del evento estará en función de la complejidad del problema encontrado,
- Esperar la indicación del Jefe de la Oficina de Tecnologías de la Información y Comunicaciones para reanudar la operación normal con las aplicaciones.

Fase de Recuperación:

Nº	Actividad	Recursos	Ejecutor	Tiempo
1	En caso existiese información pendiente de actualización, debido a la falla de los sistemas centrales, coordinar con los directores y/o jefes de áreas, para iniciar las labores de actualizaciones de los sistemas.		Jefe de la OTIC	24 horas
2	Informar a la Jefatura de la OGETIC la causa que motivo la paralización del servicio.		Jefe de la OTIC	Oportunidad : Comité
3	En función a esto, tomar las medidas preventivas del caso y revisar el Plan de Contingencia para actualizarlo en caso sea necesario.		Jefe de la OTIC	Según planificación

11. Ensayo del Plan de Contingencia

V° B° JEFATURA OGETIC

En esta fase se ensaya la reanudación de operaciones. Se valida la estrategia del Plan de Contingencia Informático.

Los objetivos que se persiguen con el ensayo del plan de contingencia básicamente son:

- Verificar si la reanudación de operaciones es adecuado y confiable para la recuperación del negocio dentro de un tiempo prudencial.
- Identificar debilidades y brechas que pudiesen existir en el plan de contingencia.

Los ensayos que se utilizarán, dependiendo de lo establecido en el plan, pueden ser:

- Lista de chequeo: Consiste en revisar la reanudación de operaciones y verificar la disponibilidad y adecuación de la información y recursos requeridos para la ejecución.
- Paseo de revisión: Se realizará previo a la conducción de un ensayo de simulación, para ello se reunirán los equipos y verbalmente describen las actividades, los procedimientos y tareas que seguirían dado un desastre.
- Simulación: Se simulará un tipo de alteración mediante un escenario de desastre. Permite a los equipos practicar la ejecución del plan de contingencia y poder validar una o más partes del plan.
- Interrupción completa: Se activará todos los componentes del plan de contingencia.

12. Vigencia

Se busca asegurar que el Plan de Contingencia Informático se mantenga actualizado, preciso y listo para ejecutarse cumpliendo los tiempos acordes.
El Plan de Contingencia Informático será revisado con una periodicidad anual para una eventual actualización y será tramitado a través de OGPP para su aprobación.
Se mantendrá una (1) copias vigentes de respaldo y se repartirá una copia digital a todas las áreas involucradas en los planes.
Se deberán hacer pruebas de los procedimientos de contingencia por lo menos semestralmente.

13. Financiamiento

Este plan se financia con cargo al Presupuesto Anual Institucional autorizado a las metas presupuestarias de los órganos y unidades orgánicas responsables de su ejecución, y no hará uso de recursos presupuestales adicionales, teniendo en cuenta que la finalidad de este es ser una hoja de ruta de acción.

14. Glosario de términos

14.1. Análisis del riesgo: Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Nota 1: El análisis del riesgo proporciona las bases para la evaluación del riesgo y para tomar las decisiones relativas al tratamiento del riesgo.
Nota 2: El análisis del riesgo incluye la estimación del riesgo.

14.2. Anonymous: Seudónimo usado mundialmente por grupos e individuos que realizan acciones de protesta en internet

14.3. Botnet: Grupo de PC's infectados y controlados por un atacante de forma remota.

14.4. Callback: Técnica de control remoto que usa la devolución de una llamada o retrollamada, en el ámbito de una telecomunicación, para tomar comando y control de un equipo

V° B° JEFATURA OGETIC

14.5. **Control**: Medida que modifica un riesgo.

14.6. **Ethical Hacking:** Práctica de ataque a infraestructuras tecnológicas para encontrar fallas de seguridad.

14.7. **Firewall:** Hardware tecnológico que brinda seguridad perimetral a la red de datos institucional.

14.8. **Gestión de continuidad del negocio**: Proceso de gestión que provee un marco conceptual para crear una salvaguarda a los objetivos de la organización incluyendo sus obligaciones.

14.9. **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

14.10. **Malware:** Cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil.

14.11. **Mensajes SMS:** mensaje de texto enviado a través del servicio de transmisión de telefonía celular.

14.12. **Ransomware:** Software malicioso que infecta equipos y da al atacante la capacidad de bloquearlo y encriptar los archivos del equipo, desde una ubicación remota

14.13. **Riesgo**: Efecto de la incertidumbre sobre la consecución de los objetivos.
Nota 1: Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.
Nota 2: Los objetivos pueden tener diferentes aspectos (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).
Nota 3: Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias, o a una combinación de ambos.
Nota 4: Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.
Nota 5: La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

14.14. **Servicio de Seguridad de EndPoint**: Tecnología de seguridad que descubre, gestiona y controla dispositivos conectados a la red de datos institucional.

14.15. **Suceso**: Ocurrencia o cambio de un conjunto particular de circunstancias.

14.16. **Switches:** Equipo de interconexión usado para conectar equipos en red.

14.17. **UPS:** Sistema de brinda una fuente alimentación eléctrica ininterrumpida, durante un periodo determinado de tiempo.

14.18. **Web Services:** servicio de intercomunicación e interoperabilidad vía web, entre equipos conectados en red.

V° B° JEFATURA OGETIC

15. Anexos

No aplica