"Año de la Universalización de la Salud"

Lima, 11 de Diciembre del 2020

RESOLUCIÓN DE PRESIDENCIA EJECUTIVA N° D000078-2020-IRTP-PE

VISTOS: El Memorando N° D0001467-2020-IRTP-OPP de la Oficina de Planeamiento y Presupuesto y el Memorando N° D0000227-2020-IRTP-OIE de la Oficina de Informática y Estadística; y,

CONSIDERANDO:

Que, mediante Decreto Legislativo N° 829 se crea el Instituto Nacional de Radio y Televisión del Perú (en adelante IRTP), es un organismo público ejecutor adscrito al Ministerio de Cultura, cuya finalidad es colaborar con la política del Estado en la educación y en la formación moral y cultural de los peruanos, teniendo como objetivo llegar a toda la población nacional, a través de los medios de radiodifusión sonora y por televisión a su cargo, con programas educativos, culturales, informativos y de esparcimiento;

Que, mediante la Resolución de Contraloría General N° 320-2006-CG, se aprueban las "Normas de Control Interno", con el objeto de propiciar el fortalecimiento de los sistemas de control interno y mejorar la gestión pública, las mismas que son aplicables a todas las entidades comprendidas en el ámbito de competencia del Sistema Nacional de Control;

Que, el numeral 3.10 de las "Normas de Control Interno" dispone que, para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación con la finalidad de mantener la continuidad del servicio, para tal efecto, 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 Oficina de Informática y Estadística mediante el Memorando N° D000227-2020-IRTP-OIE señala que remite a la Oficina de Planeamiento y Presupuesto el proyecto del "Plan de Contingencia Informático del IRTP 2020", el mismo que ha sido elaborado siguiendo un esquema ordenado y estructurado de acuerdo a los servicios informáticos que se vienen prestando en el IRTP;

Que, la Oficina de Planeamiento y Presupuesto mediante el Memorando N° D0001467-2020-IRTP-OPP señala que luego de la revisión efectuada al proyecto del "Plan de Contingencia Informático del IRTP 2020" no encuentra ninguna observación al mismo; por lo que recomienda continuar con los trámites para su aprobación;

Que, en atención a ello, resulta necesario emitir la Resolución que apruebe el "Plan de Contingencia Informático del IRTP 2020";

De acuerdo con lo dispuesto en Resolución de Contraloría General N° 320-2006-CG que aprueba las "Normas de Control Interno"; y, con el visto bueno de la Oficina de Informática y Estadística, la Oficina de Planeamiento y Presupuesto, la Oficina de Asesoría Jurídica y la Gerencia General, en el marco de las facultades conferidas por el Reglamento de Organización y Funciones del IRTP, aprobado mediante Decreto Supremo N° 056-2001-ED y modificado por el Decreto Supremo N° 006-2018-MC;

SE RESUELVE:

Artículo 1°.- Aprobar el "Plan de Contingencia Informática del Informático del IRTP 2020", que como Anexo forma parte integrante de la presente Resolución.

Artículo 2°.- Dejar sin efecto la Resolución de Presidencia Ejecutiva N° 000096-2019-IRTP-PE, que aprueba el "Plan de Contingencia Informática del IRTP 2019".

Artículo 3°.- Encargar a la Oficina de Informática y Estadística publicar la presente Resolución en el portal institucional.

Regístrese, comuníquese y cúmplase;

Documento firmado digitalmente

«EDUARDO FERNANDO GUZMAN ITURBE»
«PRESIDENTE EJECUTIVO»
I.R.T.P.

PERÚ | Instituto Nacional de Radio y Televisión del Perú | TV Perú · Radio Nacional · Radio La Crónica

PLAN DE CONTINGENCIA INFORMÁTICO

OFICINA DE INFORMÁTICA Y ESTADÍSTICA

2020

Firma Digital
INSTITUTO NACIONAL DE RADIO Y TELEVISIÓN DEL PERÚ
Firmado digitalmente por CARMONA VERGARA Benito Julio FAU 20338915471 soft
Motivo: Soy el autor del documento
Fecha: 20.11.2020 15:44:36 -05:00

Firma Digital
INSTITUTO NACIONAL DE RADIO Y TELEVISIÓN DEL PERÚ
Firmado digitalmente por ALVA TADOY Marco Antonio FAU 20338915471 soft
Motivo: Soy el autor del documento
Fecha: 26.11.2020 18:10:30 -05:00

CONTENIDO

I. OBJETIVOS 3

II. ALCANCE 3

III. BASE LEGAL 3

IV. RESPONSABILIDADES 4

V. DISPOSICIONES GENERALES 4

5.1 MATRIZ DE RIESGOS 4

5.2 PLAN DE PRUEBAS 5

VI. DISPOSICIONES ESPECÍFICAS 6

6.1 PLAN DE CONTINGENCIA RELACIONADO A LOS EQUIPOS DE COMUNICACIÓN 6

6.2PLAN DE CONTINGENCIA RELACIONADO AL CONTROLADOR DE DOMINIO 9

6.3 PLAN DE CONTINGENCIA DE RESTAURACION DEL BACKUP DE BASE DE DATOS Y CÓDIGO FUENTE DEL APLICATIVO 12

6.4 PLAN DE CONTINGENCIA RELACIONADO A LOS EQUIPOS DE TRANSMISIÓN Y SERVICIO STREAMING 15

PLAN DE CONTINGENCIA INFORMATICO 2020

I. OBJETIVOS

1.1. Servir como guía y referencia al personal de la Oficina de Informática y Estadística (OIE) ante eventos que pudieran comprometer el normal funcionamiento de los servicios informáticos definidos en el presente plan.

1.2. Garantizar la continuidad operativa de los servicios informáticos ante casos de fallas técnicas internas o externas, desastres naturales, urgencias y emergencias; estableciendo y asegurando los lineamientos para la integridad y disponibilidad 7/24/365 de los servicios y/o sistemas informáticos.

1.3. Establecer acciones y procedimientos a ejecutarse en caso de fallas en algunos de los servicios informáticos.

1.4. Garantizar la continuidad de las operaciones de los servicios informáticos considerados críticos.

1.5. Minimizar el número de decisiones que deben ser tomadas durante la duración del desastre o emergencia.

II. ALCANCE

El presente Plan de Contingencias es de estricto cumplimiento por el personal responsable de los servicios informáticos.

III. BASE LEGAL

3.1. Decreto Legislativo N° 829, “Ley de Creación del IRTP”.

3.2. Decreto Supremo N° 056-2001-ED, que aprueba el Reglamento de Organización y Funciones del IRTP y su modificatoria aprobada mediante Decreto Supremo 006-2018-MC.

3.3. Resolución de Contraloría N° 320-2006-CG, que aprueba las “Normas de Control Interno”.

3.4. Resolución Ministerial N° 004-2016-PCM, que 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 2da Edición”; en todas las entidades integrantes del Sistema Nacional de Informática.

3.5. Resolución Ministerial Nº 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

3.6. Decreto Supremo Nº 050-2018-PCM, que aprueba la definición de Seguridad Digital en el Ámbito Nacional.

IV. RESPONSABILIDADES

4.1. **Jefe de la Oficina de Informática y Estadística.-** Responsable de la supervisión y autorización de la contingencia.

4.2. **Especialista en Redes y Comunicaciones.-** Responsable de ejecutar las pruebas de las actividades del presente Plan hasta que sean totalmente satisfactorias, referidas a los Equipos de Comunicación y controlador de Dominio.

4.3. **Analista Programador.-** Responsable de ejecutar las pruebas de las actividades del presente Plan hasta que sean totalmente satisfactorias referidas al Backup de Base de Datos, Información crítica y código fuente.

4.4. **WebMaster.-** Responsable de ejecutar las pruebas de las actividades del presente Plan hasta que sean totalmente satisfactorias referidas a los Equipos de Transmisión y Servicio Streaming.

4.5. **Analista de Soporte Técnico.-** Responsable de apoyar en las actividades del presente Plan, actuando según las instrucciones del Especialista en Redes y Comunicaciones, del Analista Programador y del WebMaster.

4.6. **Oficial de Seguridad de la Información.-** Responsable de apoyar en las actividades del presente Plan, coordinando y asesorando en Seguridad de la información, brindando lineamientos que permitan reducir y mantener a un nivel aceptable los riesgos en cumplimiento de las normas.

V. DISPOSICIONES GENERALES

5.1. MATRIZ DE RIESGOS

Se ha identificado otros elementos operativos a desarrollar, estos elementos se relacionan más con las condiciones del trabajo día a día en los servicios a brindar dentro de las diferentes áreas.

Elementos operativos considerados:

5.1.1 Falla en Equipos de Comunicación.
5.1.2 Falla en controlador de Dominio.
5.1.3 Falla en la Base de Datos y Código Fuente de la Aplicación.
5.1.4 Falla en Equipos de Transmisión y Servicio Streaming.

A continuación se indica la Matriz de Probabilidad e Impacto, como base para la determinación de los niveles de riesgo de Sistemas de Información:

			GRAVEDAD (IMPACTO)		
			BAJO	MEDIO	ALTO
			1	**2**	**3**
APARICIÓN (PROBABILIDAD)	ALTA	**3**	MEDIO 3	ALTO 6	CRÍTICO 9
	MEDIA	**2**	BAJO 2	MEDIO 4	ALTO 6
	BAJA	**1**	BAJO 1	BAJO 2	MEDIO 3

Tabla 1

Resumen de la Matriz de Riesgos, considerando las contingencias relacionadas a los sistemas de información que se describirán en detalle:

Código de evento	Descripción del Evento de Contingencia	Probabilidad de Ocurrencia	Impacto	Nivel de Riesgo
OIE-01	Falla en Equipos de Comunicación	MEDIA 2	ALTO 3	ALTO 6
OIE-02	Falla en controlador de Dominio	BAJA 1	ALTO 3	MEDIO 3
OIE-03	Falla en la Base de Datos y Código Fuente de la Aplicación	BAJA 1	ALTO 3	MEDIO 3
OIE-04	Falla en Equipos de Transmisión y Servicio Streaming	MEDIA 2	MEDIO 2	MEDIO 4

Tabla 2

5.2. PLAN DE PRUEBAS

El plan de contingencia se encuentra sujeto a un cronograma para su ejecución que está definido por procedimientos a seguir, dicho cronograma se deberá cumplir hasta que las pruebas realizadas sean satisfactorias a un 100%, esto involucrará realizar el número de pruebas que se tengan que repetir para subsanar errores en el camino, para tal efecto se adoptarán acciones correctivas a fin de corregir los problemas presentados en el presente plan.

El plan de contingencia se dará por concluido al alcanzar 100% de efectividad y será cerrado con la entrega del formato de Informe Técnico al Jefe de la OIE, donde se podrá ver reflejado los resultados obtenidos de las pruebas realizadas.

El cuadro de ocurrencia de eventos del Data Center será alimentado también con los resultados obtenidos en el Informe Técnico.

El plan de pruebas correspondiente a los eventos desarrollados como parte del plan de contingencia relacionados a los elementos operativos considerados, seguirá la metodología expuesta en el presente plan.

El plan de pruebas se determinará luego del análisis de los procesos críticos del servicio y de identificar los eventos que pudieran presentarse. La aprobación del plan de pruebas será efectuada por la jefatura de la OIE previamente a su ejecución.

VI. DISPOSICIONES ESPECÍFICAS

6.1. PLAN DE CONTINGENCIA RELACIONADO A LOS EQUIPOS DE COMUNICACIÓN

6.1.1. EVENTO

OIE-01. Falla en Equipos de Comunicación

6.1.2. PLAN DE PREVENCIÓN

a) Descripción del evento

Pérdida de acceso a la red total o a un área específica en horario laborable a las estaciones de trabajo de IRTP a cargo de la OIE.

Este evento incluye los siguientes elementos mínimos identificados por la OIE, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Comunicaciones**:**

- Falla de comunicaciones Switch Core.
- Falla de los Switch de borde.

Hardware**:**

- Estaciones de trabajo

b) Objetivo

Asegurar el normal funcionamiento de la red de comunicaciones implementada por la OIE, para la comunicación entre las estaciones de trabajo y los servidores de aplicaciones de IRTP.

c) Criticidad

El nivel de riesgo de este evento es ALTO.

d) Entorno

El presente evento puede afectar a los equipos de comunicaciones (switches, ruteadores, firewall) que se encuentran instalados de acuerdo al diagrama de distribución de equipos de esta propuesta.

El cableado estructurado estará presente igualmente en todas las oficinas que cuenten con una PC conectada a los servidores de IRTP.

.

e) Personal Encargado

El personal responsable de la administración de los servicios que presta el Data Center, siendo los responsables del correcto funcionamiento de la red de comunicaciones internas durante el servicio. Coordinará las acciones necesarias para restablecer el servicio en caso se produzca un evento.

El presente Plan será supervisado por el Jefe de la OIE y contará con el apoyo del personal de Redes y Comunicaciones, y Soporte Técnico.

f) Condiciones de Prevención de Riesgo

- Contar con certificación Categoría 6 para el cableado estructurado de voz y datos de la red instalada en los ambientes de IRTP.
- Contar con un backbone certificado que interconecte las áreas del IRTP con el Data Center.
- Realizar mantenimiento periódico (cada 12 meses) a los switches.
- Solicitar al proveedor realizar el mantenimiento preventivo periódico (cada 12 meses) de los firewall, ruteadores, conectores (LC/SC) y media converter de fibra óptica usados en los servicios de internet y transacciones de datos.
- Utilizar switches y ruteadores de marcas reconocidas, que cuenten con el soporte técnico adecuado.
- Utilizar equipos que permitan el monitoreo remoto de las condiciones de funcionamiento y configuración de los switches y ruteadores.
- Contar con equipos de respaldo ante posibles fallas de los switches.
- Contar con mantenimiento preventivo para los equipos switches.

6.1.3. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

- Caída del Servidor.
- Detección de errores en la información de la Base de Datos.

b) Procesos relacionados previos del evento

Cualquier proceso relacionado a las consultas de la Base de Datos.

c) Personal que autoriza la contingencia

- Jefe de la Oficina de Informática y Estadística.

d) Descripción de las actividades después de activar la contingencia

- Verificar la causa de la falla.
- Analizar la integridad de la información.
- Buscar los archivos de respaldo requeridos
- Proceder a la restauración de la información identificada y necesaria.
- Realizar las pruebas con la información restaurada.
- Verificar el funcionamiento correcto de los servicios.

e) Duración

La duración del evento estará de acuerdo a la complejidad del problema encontrado, no debiendo ser mayor a DOS HORAS de interrupción del servicio.

6.1.4. PLAN DE RECUPERACIÓN

a) Personal encargado

El personal de Redes y Comunicaciones, luego de restablecer el equipo de comunicación, comprobará la disponibilidad de los servicios.

b) Descripción

Se informará a la Jefatura de la OIE las causas que motivaron la paralización del servicio de red. En función a esto, se tomarán las medidas preventivas del caso y se revisará el Plan de Contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se registrará en una bitácora de ocurrencias de eventos para su posterior revisión y evaluación.

d) Desactivación del Plan de Contingencia

Con la confirmación del Jefe de la OIE, se desactivará el presente Plan.

e) Proceso de actualización

En caso exista información relevante obtenida del evento producido, esta pasará a formar parte de la actualización de versiones del plan.

6.2. PLAN DE CONTINGENCIA RELACIONADO AL CONTROLADOR DE DOMINIO

6.2.1. EVENTO

OIE-02. Falla en Controlador de Dominio

6.2.2. PLAN DE PREVENCIÓN

a) Descripción del evento

Pérdida de acceso al directorio activo y/o conexión a los servidores de las estaciones de trabajo, la cual producirá una interrupción forzada en las actividades así como restringirá el acceso a los documentos de trabajo, correo electrónico institucional, carpetas compartidas, aplicativos institucionales, intranet, SIGA, SIAF integrados a la red interna.

Este evento incluye los siguientes elementos mínimos identificados por la OIE, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Comunicaciones:

- Equipos de comunicaciones

Hardware:

- Servidores
- Estaciones de Trabajo

b) Objetivo

Contar con los equipos de cómputo operativos en todo momento.

c) Criticidad

El nivel de riesgo de este evento es MEDIO.

d) Entorno

Este evento puede presentarse en las instalaciones de IRTP, tanto en la Sede TV Perú, Edificio Administrativo, Sede Radio Nacional, Almacén Central y Sede Transportes.

e) Personal Encargado

Personal responsable del correcto funcionamiento de las estaciones de trabajo de los sistemas de la OIE, de la administración de los servicios que presta el Data Center, siendo los responsables del correcto funcionamiento de la red de comunicaciones Internas durante el servicio. Coordinará las acciones necesarias para restablecer el servicio en caso se produzca un evento. El presente Plan será supervisado por el Jefe de la OIE y contará con el apoyo del personal de Soporte Técnico, Redes y Desarrollo.

f) Condiciones de Prevención de Riesgo

- Deslogeo y logeo de las estaciones de trabajo.
- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con el plan de mantenimiento preventivo y correctivo vigentes durante el servicio.
- Disponer de varios controladores secundarios que permitan distribuir los roles de Outlook.

6.2.3. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

- Fallas en la infraestructura del hardware
- Detención de las funciones de trabajo en equipos de cómputo.
- Falla de acceso a las cuentas de dominio.

b) Procesos relacionados previos al evento

Cualquier proceso relacionado con el uso de los equipos de cómputo en las instalaciones de IRTP.

c) Personal que autoriza la contingencia

- Jefe de la Oficina de Informática y Estadística

d) Descripción de las actividades después de activar la contingencia

- Asegurar que no exista problemas con la energía eléctrica.
- En caso que se encuentren problemas de funcionamiento en los equipos de cómputo, reemplazarlos con los equipos de respaldo.

e) Duración

La duración del evento estará de acuerdo de la complejidad del problema encontrado, no debiendo ser mayor a DOS HORAS de interrupción del servicio.

6.2.4. PLAN DE RECUPERACIÓN

a) Personal encargado

El personal de Redes, luego de restaurada la falla en los controladores de dominio (Active Directory) y/o servidores, coordinará con los usuarios, para la reanudación de los trabajos operativos en las instalaciones del IRTP.

b) Descripción

Se informará a la Jefatura de la OIE la causa del problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el Plan de Contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la Coordinación Ejecutora del Plan para su revisión.

d) Desactivación del Plan de Contingencia

Con la confirmación del Jefe de la OIE, se desactivará el presente Plan.

e) Proceso de actualización

En base al informe presentado que identifica las causas de la falla del servidor y/o Active Directory, se determinara las acciones preventivas necesarias que deben incluirse en el siguiente plan.

6.3. PLAN DE CONTINGENCIA DE RESTAURACIÓN DEL BACKUP DE BASE DE DATOS Y CÓDIGO FUENTE DEL APLICATIVO

6.3.1. EVENTO

OIE-03. Falla en la Base de Datos y Código Fuente de la Aplicación

6.3.2. PLAN DE PREVENCIÓN

a) Descripción del evento

Posible falla en la base de datos y el código fuente de la aplicación, suspenderá el uso de los sistemas de información. Este evento puede ser originado por:

- Manipulación del código fuente e información de la base de datos.
- Virus Informático.
- Caída del servidor de aplicaciones y base de datos.

El evento incluye los siguientes elementos mínimos identificados por la OIE, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware:

- Servidores de Aplicaciones y Base de datos
- Estaciones de Trabajo (PC)
- Energía eléctrica.
- Consumo total del disco asignado al backup por falta de eliminación periódica de historial.

Software:

- Inoperatividad de los aplicativos de la entidad.
- Falla en la configuración de restauración del backup.

Incidencias comunes:

- Pérdida de información:
  Debido a que no se culminó una transacción

- Información no confiable:
  Manipulación indebida interna y/o externa de la información

- Acceso a la información:
  Limitaciones para realizar consultas y/o transacciones
  Falla en la programación de consultas

b) Objetivo

Garantizar la disponibilidad y salvaguardar la integridad de toda la información.

c) Criticidad

El nivel de riesgo de este evento es ALTO.

d) Entorno

Este evento puede presentarse en las instalaciones de IRTP, tanto en la Sede TV Perú, Edificio administrativo, Sede Radio Nacional, Almacén Central y Sede Transportes.

e) Personal Encargado

Personal responsable del correcto funcionamiento y administración de la Base de Datos. Coordinará las acciones necesarias para restablecer el servicio en caso se produzca un evento. El presente Plan contará con el apoyo del personal de Soporte, Redes y Desarrollo.

f) Condiciones de Prevención de Riesgo

- Limitar el acceso a la base de datos y servidor de aplicaciones.
- Utilizar un estándar de programación y base de datos.
- Realizar diariamente Backup de la base de datos y aplicativo.
- Contar con un servidor y/o plataforma de respaldo de la base de datos y aplicaciones.

6.3.3. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

- Caída del Servidor de aplicaciones y base de datos.
- Manipulación del código fuente e información de la base de datos.
- Detección de errores en la información de la Base de Datos.

b) Procesos relacionados previos del evento

- Funcionalidades del sistema de información que realiza transacciones o consultas a la Base de Datos.

c) Personal que autoriza la contingencia

- Jefe de la Oficina de Informática y Estadística.

d) Descripción de las actividades después de activar la contingencia

- Verificar la causa del problema.
- Buscar los archivos de respaldo requeridos.
- Restaurar los backup de la base de datos y aplicativo.
- Analizar la integridad de información de la base de datos.
- Realizar las pruebas funcionales del sistema de información.
- Verificar de manera integral el correcto funcionamiento del sistema de información.

e) Duración

La duración del evento estará de acuerdo de la complejidad del problema encontrado, no debiendo ser mayor a DOS HORAS de interrupción del servicio.

6.3.4. PLAN DE RECUPERACIÓN

a) Personal encargado

Luego de restablecer los sistemas de información y base de datos, estos serán enviados a producción por el personal de Desarrollo.

b) Descripción

Se informará a la Jefatura de la OIE las causas que motivaron la restauración de la información. En función a esto, se tomarán las medidas preventivas del caso y se revisará el Plan de Contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se registrará en una bitácora de ocurrencias de eventos para su posterior revisión y evaluación.

d) Desactivación del Plan de Contingencia

Con la confirmación del Jefe de la OIE, se desactivará el presente Plan.

e) Proceso de actualización

En caso exista información relevante obtenida del evento producido, esta pasará a formar parte de la actualización de versiones del plan.

6.4. PLAN DE CONTINGENCIA RELACIONADO A LOS EQUIPOS DE TRANSMISIÓN Y SERVICIO STREAMING

6.4.1. EVENTO

OIE-04. Falla en Equipos de Transmisión y Servicio Streaming

6.4.2. PLAN DE PREVENCIÓN

a) Descripción del evento

La pérdida de acceso a los equipos de transmisión y servicio Streaming producirá una interrupción forzada de la transmisión de las señales de TV Perú, Canal IPE y/o Radio Nacional por internet.

Este evento incluye los siguientes elementos mínimos identificados por la OIE, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Comunicaciones

- Falla de comunicaciones de los accesos a red.

Hardware

- Estaciones de transmisiones.

Servicios

- Servicio de Transmisión Streaming.

Equipos de captura (Supervisado y Administrado por la Gerencia Técnica)

- Equipo distribuidor de Video de Televisión (OpenGear DFR 8321)
- Cable de video SDI que conecta la Estación de transmisión con el equipo de distribución de Video
- Equipo de Audio de Radio Nacional (Consola de Audio Lawo Sapphire)
- Equipo de Audio de Radio La Crónica (Consola de Audio Allen & Heath ZED-22)

b) Objetivo

Garantizar la operación de los equipos de transmisión con los índices de calidad del servicio establecidos para la transmisión de la señal de TV/Radio, sin fallas ni errores en la transmisión, asegurando una óptima calidad en imagen y audio, así mismo atendiendo en los casos de los transmisores de TV y Radio la cobertura prevista.

c) Criticidad

El nivel de riesgo de este evento es MEDIO.

d) Entorno

El presente evento puede afectar las prestaciones del Portal Web y compromisos en emisión de contenidos Streaming.

e) Personal Encargado

El personal responsable de la administración de los servicios que presta la transmisión Streaming, siendo los responsables del correcto funcionamiento del servicio. Coordinará las acciones necesarias para restablecer el servicio en caso se produzca un evento. El presente Plan será supervisado por el Jefe de la OIE y contara con el apoyo del personal de Redes, Soporte Técnico y Portal Web.

f) Condiciones de Prevención de Riesgo

- Contar con certificación Categoría 6 para el cableado estructurado de voz y datos de la red instalada en los ambientes de IRTP.
- Realizar mantenimiento periódico (cada 12 meses) a los equipos de transmisión.
- Solicitar al proveedor Streaming realizar el monitoreo constante para el correcto funcionamiento del servicio.
- Utilizar equipos que permitan el monitoreo remoto de las condiciones de funcionamiento.
- Contar con equipos de respaldo que funcionen como imagen de los equipos operativos.
- Contar con un servicio de respaldo.
- Disponer de equipos de monitoreo del servicio.

6.4.3. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

- Falla en el servicio de trasmisión a través del portal web correspondiente.
- Falla de acceso al equipo de transmisión.
- Fallas en el servicio de transmisión a través del portal web correspondiente.

b) Procesos relacionados previos del evento

- Cualquier proceso relacionado con el uso del servicio de transmisión Streaming.
- Cualquier proceso relacionado con la caída del servicio Streaming.

c) Personal que autoriza la contingencia

- Jefe de la Oficina de Informática y Estadística

d) Descripción de las actividades después de activar la contingencia

- Verificar la causa de la falla.
- En el caso del equipo de transmisión, asegurar que no exista problemas con la energía eléctrica y/o conexión de la captura de Audio y Video.

- En caso que se encuentren problemas de funcionamiento en los equipos de cómputo, reemplazarlos con los equipos de respaldo.
- Realizar las pruebas de captura y emisión de la señal.
- Verificar el funcionamiento correcto del servicio.
- Contactar con el proveedor responsable de brindar el servicio Streaming.

e) Duración

La duración del evento por falla de la estación de transmisiones estará en función de la complejidad del problema encontrado, no debiendo ser mayor a DOS HORAS de interrupción del servicio, tiempo que fue o será definido en las pruebas de contingencia programadas.

La duración del evento por fallas del Servicio de Transmisión Streaming estará de acuerdo de la complejidad del problema detectado por el proveedor, no debiendo ser mayor a la garantía del servicio de 99.95% anual.

6.4.4. PLAN DE RECUPERACIÓN

a) Personal encargado

El Personal del Portal Web, luego de restituida la operación del equipo de transmisión y/o servicio, coordinará con los usuarios de la Gerencia de Televisión, para la reanudación de la trasmisión Streaming a través de los portales web correspondientes.

b) Descripción

Se informará a la Jefatura de la OIE las causas que motivaron la paralización del servicio Streaming. En función a esto, se tomarán las medidas preventivas del caso y se revisará el Plan de Contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se registrará en una bitácora de ocurrencias de eventos para su posterior revisión y evaluación.

d) Desactivación del Plan de Contingencia

Con la confirmación del Jefe de la OIE, se desactivará el presente Plan.

e) Proceso de actualización

En caso exista información relevante obtenida del evento producido, esta pasará a formar parte de la actualización de versiones del plan.