GOBIERNO DE EL SALVADOR

MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

PLAN DE CONTINGENCIA PARA LA CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS DEL MINISTERIO DE TRABAJO Y PREVISIÓN SOCIAL

UNIDAD DE DESARROLLO TECNOLÓGICO

2021

AUTORIZÓ:

Oscar Rolando Castro
Ministro de Trabajo y Previsión Social

VISTO BUENO:

Marvin Humberto Juárez López
Director Ejecutivo.

ELABORÓ:	REVISÓ:
William Caleb Cerón Arias Jefe Unidad de Desarrollo Tecnológico	Enrique Paz Jefe de la Oficina de Coordinación y Desarrollo Institucional

Contenido

Antecedentes

El Ministerio Trabajo y Previsión Social considera que la información es el patrimonio principal de toda la institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar cualquier eventualidad o desastres de diversos tlpos.

Este plan de contingencia tiene como objetivo garantizar la prestación de servicios a la ciudadanía en general y la protección de la información del Ministerio de Trabajo y Previsión Social ante posibles riesgos a los que puedan estar expuesto los equipos de cómputos o sistemas de información utilizados en la institución. Corresponde a la Unidad de Desarrollo Tecnológico, aplicar medidas de seguridad para proteger y prevenir contingencias y desastres de diversos tipos que atenten al buen funcionamiento de los sistemas de información o equipos informáticos considerados como críticos en la Entidad.

Los sistemas de información son para la institución un importante avance en la materia de modernización de los servicios ofrecidos a la ciudadanía y a las áreas internas de la institución.

Por todo lo anterior y ante las amenazas existentes en el mundo tecnológico que buscan causar daño a la ciudadanía en general o sabotear la gestión del Estado a través del robo de información o la suspensión de los servicios, la Unidad de Desarrollo Tecnológico ha definido las acciones que se deben seguir al momento de presentarse una eventualldad, con el fin de mantener o reestablecer las funciones Tecnológicas de la información y la comunicación del Ministerio en el menor tiempo posible, teniendo en cuenta la disponibilidad de recursos físicos y humanos actuales; relacionados en el presente documento.

Objetivo general

Garantizar la continuidad de las TIC · S del Ministerio de Trabajo y Previsión Social, ante la presencia de eventos que puedan alterar el normal funcionamiento de los sistemas de información o equipos informáticos considerados como críticos en la Entidad, restableciendo el servicio en el menor tiempo posible, a través de la puesta en marcha de procedimientos, actividades y elementos requeridos para afrontar eventualidades que alteren el funcionamiento correcto de los mismos.

Objetivos específicos

i. Mantener la prestación de los servicios informáticos del Ministerio de Trabajo y Previsión social.
ii. Definir actividades y procedimientos a ejecutar en caso de una interrupción de las operaciones de los sistemas y/o procesos que involucren la infraestructura de TI del Ministerio de Trabajo y Previsión Social a fin de garantizar la continuidad en la ejecución de los objetivos estratégicos de la entidad en el menor tiempo posible.
iii. Mantener accesibles los sistemas de información críticos de la entidad cuando sean interrumpidos o paralizados por eventos que puedan alterar el normal funcionamiento que afecten parcial o totalmente las instalaciones donde se procesan los sistemas y los servicios de datos de la Entidad.
iv. Identificar y analizar posibles riesgos que pueden afectar las operaciones y procesos informáticos de la institución.
v. Preparar y organizar al personal de la Unidad de Desarrollo Tecnológico para afrontar adecuadamente las eventualidades o incidencias que alteren el correcto funcionamiento de los servicios informáticos del Mlnisterio de Trabajo.

Normativa Legal.

a) Normas Técnicas de Control Interno.
b) Ley Especial Contra Los Delitos Informáticos y Conexos.
c) Políticas y Procedimientos de los Controles Generales de los Sistemas de Información

Alcance.

El Plan de Contingencia de la Unidad de Desarrollo Tecnológico del Ministerio de Trabajo y Previsión Social, contiene las acciones para el manejo de riesgos a la infraestructura de Hardware. Software y Equipos de comunicaciones involucrados en los sistemas de información críticos de la institución. Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales del centro de datos de la institución.

Términos y definiciones.

Contingencia: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

Riesgo: Posibilidad *de* que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Amenaza: Posible peligro que una situación, un objeto o una circunstancia especffica puede conllevar para la vida, de uno mismo o de terceros o de un sistema. Es un peligro que está latente, que todavía no se ha desencadenado pero que sirve como aviso para prevenir o para presentar la posibilidad de que sí lo haga. Posibilidad de ocurrencia de un suceso.

Vulnerabilídad: Es el grado de pérdida de un elemento o grupo de elementos. Nivel de ser susceptible a sufrir un daño o lesión por la ocurrencia de un peligro o amenaza.

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilízan como sinónimos.

Incidente: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

Activo: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimlento y reputación en el mercado.

Plan de Contingencias: Plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad

Caídas leves: son perdidas del suministro de energía eléctrica de corta duración, fallas en disco duros, etc.

Caídas Severas: destrucción de equipos por terremotos, incendios, etc.

Líder: responsable de generar el plan de contingencia y toma de decisiones.

Coordinador: dirigir y promover el desarrollo integral e implementación del plan de contingencia informático, así como verificar el cumplimiento de las actividades asignadas al equipo de emergencia.

Equipo de emergencia: responsable de configurar los elementos necesarios (programas, equipo, entre otros) para los sistemas críticos se restablezcan en un sitio alterno antes de que se cumpla el tiempo máximo de restablecimiento.

Equipo de apoyo externo: personal de apoyo de otras unidades, el proceso de comunicación será por medio de la jefatura de UDT con el resto de oficinas de las cuales se requiera algún servicio.

Proceso Crítico: proceso considerado indispensable para la continuidad de la operación y servicios de la institución, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativopara la institución.

Sitlo Alterno Tibio (warn Stamdby): son ambientes equipados parcialmente con hardware, software, equipos de telecomunicaciones y electricidad; y que además se mantienen en estados operativos.

Usuario: individuo que utiliza una computadora, sistema operativo o un sistema de información, el cual se asocia en una cuenta única de usuario para acceder a un servicio a través de un inicio de sesión.

Proveedor: Persona o empresa que abastece a otras empresas o personas con productos, bienes o servicios, los cuales serán transformados para venderlos posteriormente y/o directamente se compran para su venta.

Centro de procesamiento: Ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Dichos recursos

consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones. Un CPD es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Virtualización: Es la creación a través de software, de una versión no física de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

Desastre: Es un evento calamitoso, repentino o previsible, que trastorna seriamente el funcionamiento de una comunidad, sociedad u organizaclón y causa pérdidas humanas, materlales, económicas o ambientales que desbordan la capacidad de la comunidad o sociedad afectada para hacer frente a la situación a través de sus propios recursos. Aunque frecuentemente están causados por la naturaleza, los desastres pueden deberse a la actividad humana.

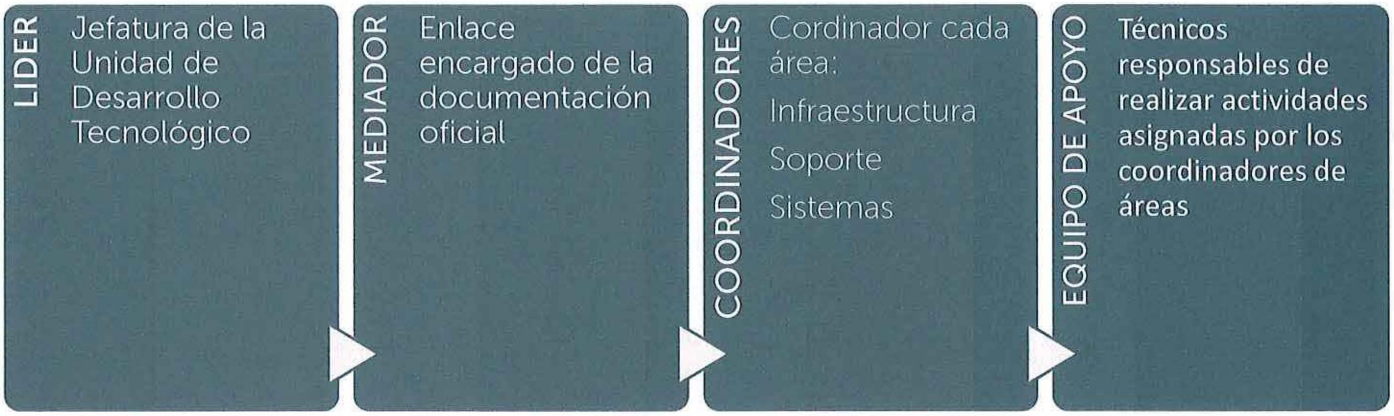
Estructura del Plan de Contlngencias

En esta sección se presentarán las actividades a realizar para la elaboración del presente Plan. Se llevarán a cabo las siguientes actividades:

» Organización roles y responsabilidades.
» Identificación y priorización de los riesgos.
» Análisis y clasificación de los riesgos.
» Inventario de hardware, software y Sistemas de Información
≫ Actividades del plan según el riesgo.
» Procedimiento del Plan de Contingencias de TI
» Actualización del Plan de Contingencias de TI

ESTRUCTURA FUNCIONAL DEL PLAN DE CONTINGENCIA PARA LA CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS DEL MTPS

Para el desarrollo e implementación del presente Plan, se ha diseñado la siguiente estructura. definiendo las responsabilidades por cada una de las personas participantes.



Líder: Nombre: Lic. William Caleb Cerón Arias
Cargo: Jefe de la Unidad de Desarrollo Tecnológico.

Mediador: Nombre: Inga. Alma Stephanie Portillo Rivera
Cargo: Técnico de la Unidad de Desarrollo Tecnológico.

Coordinadores: Nombre: Téc. José Franklin Pineda Barahona
Cargo: Coordinador del Área de Infraestructuray Telecomunicaciones.

Nombre: Téc. Angel William Cruz
Cargo: Técnico del Área Soporte Técnico.

Nombre: lng. William Ernesto Rivera Guerrero
Cargo: Coordinador del Área de Desarrollo Sistema.

Equipo de Apoyo:

Área de Infraestructura y Telecomunicaciones:
Nombre: Cesar Ramón Linares
Robin Antonio Medina
Blanca Ramirez
Napoleón Ernesto Escalante
Joel Flores

Área Soporte Técnico
Nombre: Angel Cruz
Manuel Molina

Área de Desarrollo Sistema
Nombre: William Medrana
Vladimir Sánchez
Antonio Castro
Henry Pérez

Responsabilidades

Líder

- Dirigir y promover el desarrollo integral *e* implementación del Plan de Contingencia Informático, así como verificar el cumplimiento de las activídades encargadas a cada uno de los responsables.

Mediador

- Velar por que todos los participantes del proyecto sigan el plan de trabajo establecido.
- Verificar y efectuar el seguimiento para que el plan sea expresado en documentos formales y de fácil entendimiento.
- Informar al líder, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

- Identificar los responsables por cada área, así como las prioridades para el desarrollo de las tareas.
- Establecer coordinaciones entre el Equipo de Trabajo, el Líder de Equipo y las demás Unidades Organizativas involucradas.
- Socializar los objetivos, alcances, acciones y resultados de la ejecución del plan.

Coordinadores

- Identificar los problemas, desarrollar y recomendar las soluciones establecidas en este plan y comunicar al coordinador aquellas acciones específicas que *se* ejecutarán y no están contempladas en este plan.
- Ejecutar las acciones determinadas en el cronograma o plan de trabajo, cumpliendo los plazos señalados a fin de no perjudicar el cumplimiento de las demás tareas.
- Comunicar oportunamente al coordinador, sobre los avances de las tareas asignadas, así como las dificultades encontradas y la identificación de los riesgos.
- Identificary registrar los aspectos operativos no contemplados en el cronograma de actividades.
- Ejecutar las acciones correctivas del caso, coordinando su implementación con el coordinador.
- Solicitar apoyo y delegar actividades al equipo de emergencia de la Unidad de Desarrollo Tecnológico que se encuentren en su área.
- Organizar y orientar al equipo de trabajo de su área que tiene asignadas actividades para el cumplimiento del plan de contingencia.

Equipo de Emergencia

- Apoyar en las actividades asignadas por los coordinadores para el cumplimiento del plan de contingencia.
- Ejecutar las acciones determinadas en el cronograma o plan de trabajo, cumpliendo los plazos señalados a fin de no perjudicar el cumplimiento de las demás tareas.

- Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- Participaren las actividades de continuldad (Capacitaciones, divulgación, pruebas y ejecución)

IDENTIFICACIÓN Y PRIORIZACIÓN DE RIESGOS

Externos

Incumplimiento al objeto contractual por parte de los contratistas.
Riesgo externo que consiste en el atraso que puede presentar la ejecución o trasgresión del clausulado de los contratos de actualización, modificación, mantenimiento y soporte del hardware, software por deficiencias en el desarrollo precontractual y/o por deficiencias en la supervisión del contratos que involucren a los sistemas de información catalogados como críticos, que al presentarse genera inoperancia de los sistemas de información o mala imagen de la entidad por aplicativos desactualizados. Tipo de riesgo: Cumplimiento.

Caída o interrupción del sistema eléctrico
Riesgo externo. Corresponde al corte del servicio de energía eléctrica en el Ministerio de Trabajo y Previsión Social por parte de falla externa en el proveedor del servicio, corte eléctrico que genera Interrupción del funcionamiento de los equipos donde se alojan los aplicativos críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnología.

Caída del canal de internet
Riesgo externo. Consiste en las fallas técnicas por parte del proveedor del servicio de internet en el Ministerio de Trabajo y Previsión Social, lo que ocasionaría suspensión de los servicios de correo y de los aplicativos críticos de la entidad. Tipo de riesgo: Tecnológico.

Caída del Servicio Telefónico
Riesgo externo correspondiente a la suspensión del servicio por daños o fallas en el software o hardware de telefonía IP de telefonía en el Ministerio de Trabajo y Previsión

Social., que de presentarse genera la ausencia de comunicación telefónica en la entidad. Tipo de riesgo: Tecnológico

Caída de servicios por virus informático
Riesgo externo. Es el riesgo de infección de los equipos servidores y 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 un servicio de red, inoperancia o inestabilidad de los sistemas. Tipo de riesgo: Tecnológico.

Suspensión del servicio por sismo, inundación o incendio
Riesgo externo. Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo, inundación o incendio que afecte la infraestructura tecnológica de los sistemas de información críticos del Ministerio de Trabajo y Previsión Social, generando suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia de los sistemas o inestabilidad de los mismos. Tipo de riesgo: Operativo.

Internos

Retrasos en el Proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad.
Riesgo interno que corresponde a retrasos en el proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad por deficiente planeación del proceso de contratación, falta de personal capacitado para realizar los estudios previos de contratación. Lo que puede ocasionar Inoperancia de los sistemas de información, desactualización de los sistemas de información. Tipo de riesgo: Operativo

Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción.
Riesgo interno que tiene baja probabilidad de ocurrencia y consiste en el robo. alteración o extracción de la información que es considerada confidencial o clasificada como reservada por deficiencia en las políticas de seguridad o Configuración ineficiente del cortafuegos de la entidad. Al materializarse, el impacto es negativo ya que puede

ocasionar demandas y sanciones a laentidad, mala imagen institucional.Tipo de riesgo: Tecnología.

Falla técnica en equipos servidores, de escritorio o de comunicaciones.
Riesgo interno que corresponde al daño físico o lógico de un equipo servidor, de escritorio o de comunicaciones que afecta el funcionamiento de un sistema de información crítico o de servicio por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los usuarios que hace que el servicio quede inoperante o Inestable. Tipo de riesgo: Tecnológico

Falla técnica en sistemas de información.
Riesgo interno, corresponde al riesgo de presentarse errores de lógica en programación o incompatibilidad entre software que afectan a los sistemas de información que genera Inoperancia o inestabilidadde los sistemas de información. Tipo de riesgo: Tecnológico.

ANÁLISIS Y CLASIFICACIÓN DE LOS RIESGOS

Los riesgos de seguridad de la información del Ministerio de Trabajo y Previsión Social, se clasifican para elaborar y realizar monitoreo y seguimiento al mapa de riesgos institucional.

La Calificación del Riesgo: Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse y la segunda se refiere a la magnitud de sus efectos.

Se puede medir con criterios de:

1. Frecuencia, si se ha materializado.

2. Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo.

Matriz de evaluación de riesgos

Probabilidad	Descripción	Frecuencia	Valor
Casi seguro	El evento probablemente ocurriría en la mayoría de los casos	Más de una vez al año	5
Probable	El evento probablemente ocurriría en la mayoría de los casos	Al menos una vez en el último año	4
Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años	3
Improbable	El evento podría ocurrir en algún momento	Al menos una vez en los últimos cinco años.	2
Raro	El evento podría ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos cinco (5) años	1

Probabilidad: Posibilidad de ocurrencia del riesgo.

Impacto	Descripción	Valor
Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad: - Pérdida de recursos secundarios. - Disminución del rendimiento de los procesos de negocio de MTPS. - Pérdida de información interna no publicada. - Suspensión de los sistemas críticos. - Pérdida de información confidencial estratégica. - Deterioro de la imagen institucional.	5

Impacto	Descripción	Valor
Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad. - Investigaciones - Sanciones - Demandas	4
Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.	3
Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.	2
Insignificante	Si el hecho llegará a presentarse tendría consecuencias o efectos mínimos sobre la Entidad: - Pérdida de recursos críticos pero que cuentan con elemento de respaldo. - Caída notable del rendimiento de los procesos de negocio del MTPS (SNIT. VISAS H2A, SIE. SITIO WEB,..). - Pérdida de información confidencial pero no considerada estratégica. - Suspensión temporal del servicio.	1

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

La Evaluación del Riesgo: permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos EXTREMOS, ALTOS, MODERADOS, BAJOS y fijar las prioridades de las acciones requeridas para su tratamiento.

CLASIFICACIÓN DE LOS RIESGOS

Riesgo	**Incumplimiento al objeto contractual por parte de los contratistas.**
Probabilidad	Probable
Impacto	Moderado
Efecto	Perdida de servicios de telecomunicación, perdida de comunicación entre oficinas por falla en equipos de seguridad perimetral, perdida de información por ataques de virus por incumplimiento del proveedor .
Medidas de Previsión	Monitoreo constante de los servicios contratados
Acciones de Previsión y Recuperación	Realizar los procedimientos para determinar si el problema es del proveedor o del MTPS Coordinar con la empresa para recuperación del servicio

Riesgo	**Caída o interrupción del sistema eléctrico**
Probabilidad	Casi Seguro
Impacto	Mayor
Efecto	Paralización total de las actividades del MTPS, servicios restringidos, se mantendrá la operatividad con servicios mínimos.
Medidas de Previsión	Realizar mantenimiento a UPS centralizado.
Acciones de Previsión y Recuperación	Poner en funcionamiento la fuente de energía alterna (ups centralizado) para el centro de datos.

Riesgo	Caída del canal de internet
Probabilidad	Probable
Impacto	Mayor
Efecto	Imposibilidad al acceso de internet y sistemas informáticos Perdida de comunicación por medio de vpn a las oficinas departamentales

Medidas de Previsión	Verificar el funcionamiento de los dos enlaces de internet
Acciones de Previsión y Recuperación	Realizar los procedimientos para determinar si el problema es del proveedor o falla en los equipos de comunicación Coordinar con la empresa de telecomunicaciones la reposición del servicio o enmendar la falla del equipo de comunicaciones.

Riesgo	Caída del Servido Telefónico
Probabilidad	probable
Impacto	moderado
Efecto	Perdida de comunicación y call center
Medidas de Previsión	Solicitar mantenimiento al proveedor del servicio Realizar respaldo de la planta telefónica
Acciones de Previsión y Recuperación	Realizar los procedimientos para determinar si el problema es del proveedor. Restablecer el respaldo realizado

Riesgo	Caída de servicios por virus informático
Probabilidad	probable
Impacto	catastrófico
Efecto	Pérdida *de* recursos secundarios. Disminución del rendimiento de los procesos de negocio de MTPS. Pérdida de información interna no publicada.
Medidas de Previsión	Mantener actualizado los antivirus de los equipos informáticos. Restringir el libre uso de usb. al ser los principales medios de contaminación.

Acciones de Previsión y Recuperación	Aislar el equipo contaminado Verificar equipos daños Restauración de respaldo de equipos dañados

Riesgo	**Suspensión** del servicio **por sismo, inundación o incendio**
Probabilidad	probable
Impacto	catastrófico
Efecto	Posible deterioro/ inutilización de las instalaciones del MTPS En casos muy graves, inutilización total de servidores de aplicaciones y equipos de comunicación
Medidas de Previsión	Entrenamiento del personal para asumir funciones en casos de desastres Sistemas de extinción de fuego Verificar que los extintores se encuentren vigentes
Acciones de Previsión y Recuperación	Verificar si el sitio de contingencia *se* encuentre en óptimas condiciones Llamar a las unidades de bomberos Desconectar fuentes de energía del centro de datos Verificar el funcionamiento de los equipos del centro de datos

Riesgo	**Retrasos en el Proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad.**
Probabilidad	Probable
Impacto	catastrófico

Efecto	Perdida de comunicación de servlcl0s, perdida de información por ataques de virus.
Medidas de Previsión	Verificaciones constantes de los servicios contratados
Acciones de Previsión y Recuperación	Realizar los procedimientos para determinar si el problema es del proveedor o del MTPS Coordinar con la empresa para recuperación del servicio

Riesgo	**Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción.**
Probabilidad	posible
Impacto	catastrófico
Efecto	divulgación de información confidencial
Medidas de Previsión	actua lízación de antivirus, bloqueo de usb o dispositivos de almacenamiento
Accíones de Prevísión y Recuperación	Restauración de respaldo del sistema información

Riesgo	Falla técnlca en equipos servidores, de escritorio o de comunicaciones.
Probabilidad	posible
Impacto	moderado
Efecto	Caída notable del rendimiento de los procesos de negocio del MTPS
Medidas de Previsión	Contar que los equipos tengan garantía Monitoreo constante de los equipos
Acciones de Previsión y Recuperación	Verificación de servidores, restauración de respaldos

Riesgo	Falla técnica en sistemas de información.
Probabilidad	Posible
Impacto	moderado

Efecto	Caída notable del rendimiento de los procesos de negocio del MTPS
Medidas de Previsión	Realizar respaldos
Acciones de Previsión y Recuperación	Verificación del error que muestra el aplicativo, realizar el mantenimiento correctivo.

INVENTARIO DE SERVIDORES

SERVIDOR	PRIORIDAD
Servidor de Base datos SN !T	ALTA
Servidor de Base de Datos SIE	ALTA
Servidor de Active Directory Principal	ALTA
Servidor de Sitio RenacEmpleo	ALTA
Servidor de Base de Datos para Sitio Cálculos, Citas y otros.	ALTA
Servidor de Base de Datos del Sitio Visa	ALTA
servidor de base de datos de aplicativos en desarrollo	ALTA
servidor de Base de Datos del SN IT	ALTA
Servidor de Sitio InstitucionalActual	ALTA
VMware vCenter Server Appliance	ALTA
vSphere Replication Appliance	ALTA
Servidor DHCP	ALTA
Servidor de Keycloak para desarrollo	BAJA
Servidor para el registro de marcaciones de asistencia	BAJA
Sincroniza el directorio de Active Directory con Office 365 online	MEDIO
Servidor de AntiSPAM	MEDIO
Servidor para los sitios cálculos y cita	MEDIO
Servidor del Sitio para Portal de Servicios	MEDIO
Servidor para servicios internos.	MEDIO
Servidor de Administración citas y calculadoras Interno	MEDIO
Servidor para sitio Covid19	MEDIO
Servidor de recursos compartidos	MEDIO
Servidor para carpetas compartidas solo Recursos Humanos	MEDIO
Servidor de aplicativos Internos	MEDIO
Servidor de Sitio SN IT	MEDIO
Servidor de Sitio SNAT	MEDIO
Consola de Administración de Antivirus Sophos	MEDIO
Servidor para Sitio Visa Publico	MEDIO
Servidor de correo Institucional	MEDIO

INVENTARIO DE PROGRAMAS INFORMATICOS

N°	NOMBRE DEL PROGRAMA INFORMATICO	DESCRIPCION	PRIORIDAD
1	Sistema Nacional de Notificaciones de Accidentes de Trabajo	Registrar las notificaciones de accidentes de trabajo ocurridas en las empresas o en el trayecto hacia o desde las mismas.	Alta
2	Renacempleo {Registro de ofertas de empleo por parte de los gestores)	Registrar la vinculación entre empresas y población en busca de una oportunidad laboral.	Alta
3	Sistema de Gestión de Recursos Humanos	Registrar información básica de los empleados de la institución, así como también datos laborales, niveles académicos, licencias, información de familiares y capacitaciones.	Baja
4	Sistema de Gestión de Solicitudes de Vehículo	Agilizar el proceso de solicitudes de misiones oficiales. Mejorar reportes de consumo y asignación de vales, a fin de validar la liquidación con contabilidad, garantizando la fiabilidad de la información generada.	Baja
5	Sistema de Gestión de Activo Fijo	Registrar información relacionada a los activos de la institución, para calcular las depreciaciones y movimientos físicos de los mismos.	Baja
6	Sistema de Gestión de Bodega	Registrar la entradas y salidas de los productos administrados por Bodega Institucional. para generar información que es insumo para la ejecución contable, y la toma de decisiones.	Baja
7	Sistema de Evaluación de Desempeño de Personal	Gestionar y mantener el registro de evaluaciones de personal de acuerdo	Baja

N°	NOMBRE DEL PROGRAMA INFORMATICO	DESCRIPCION	PRIORIDAD
		a los perfiles de evaluación aprobados para cada evento.	
8	Sistema Nacional de Inspección de Trabajo	Registrar la información que se genera en el proceso de inspección y automatizar el proceso que vigila el cumplimiento de la normativa laboraL	Alto
9	Sistema de Gestión de Viáticos y Pasajes al Interior	Automatizar la gestión de viáticos y visitas al interior de las personas empleadas de esta institución.	Baja
10	Sitio Web Institucional	Facilitar una herramienta de divulgación del que hacer institucional que pueda ser accedido desde diferentes dispositivos con acceso a internet.	Alta
11	Intranet	Proporcionar al personal de la institución, información y documentación que sirve como apoyo a la realización de las labores.	Baja
12	Sistema de Soporte	Registrar las actividades de soporte técnico y mantenimiento ejecutado por el personal de la Unidad de Desarrollo Tecnológico, en lo relativo: Sistemas, soporte técnico, redes, y gestión de TI	Baja
13	Sistema de Gestión de Credenciales de los Sistemas Informáticos	Gestionar la seguridad de los sistemas, módulos, roles y usuarios de los sistemas integrados en el ERP institucional.	Baja
14	Sistema de VISAS	Facilitar la inclusión laboral de salvadoreños a través de la migración regular, ordenada y segura hacia países donde se identifiquen oportunidades de empleo. Las	Alta

N°	NOMBRE DEL PROGRAMA INFORMATICO	DESCRIPCION	PRIORIDAD
		empresas extranjeras deben respetar los derechos laborales de los salvadoreños y proporcionar igualdad de condiciones que los ciudadanos de esas naciones	
15	Sistema de Registro Citas	Es el encargado de realizar citas para que los usuarios sean atendidos en la institución	Alta
16	Sistema de Cálculo	Es el que se encarga de realizar el cálculo monetario de indemnización de los usuarios	Alta
17	Sistema de Denuncias	Es donde se registran las denuncias de violaciones laborales de los usuarios	Alta
18	Slstema de autentificación de los aplicativos	Sistema de inicio de sesión único y registro los empleados Institucionales y usuarios externos para que accedan a los diferentes aplicativos	Alta
19	Sistema de Directorio Institucional	Registrar el contacto telefónico, celular y correo de los Empleados Institucionales	Baja
20	Sistema de Marcación	Consultar las marcaciones de asistencias de entrada y salida de los empleados Institucionales en las diferentes oficinas por los relojes marcadores.	Baja

ACTIVIDADES SEGÚN RIESGOS

#	RIESGOS	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO
1	Incumplimiento al objeto contractual por parte de los contratistas.	• Se comunica inmediatamente con el proveedor para hacer efectiva el contrato, o el servicio adquirido por medio del contrato	Administrador de Contrato
2	Caída o interrupción del sistema eléctrico	• Verificación centro de datos • Verificación del U PS centralizado • Verificación de aire centralizado • Contactar a Dirección Administrativa para que se realice la comunicación con el distribuidor de energía eléctrica. Si la interrupción de energía eléctrica tiene una duración de más de 1 hora 30 minutos se realizarán las siguientes actividades: • Apagado del sistema de respaldo • Apagado de máquinas virtuales • Apagado de servídores físicos en producción • Apagado del sistema de almacenamiento	Dirección Administrativa William Ceron Franklin Pineda Blanca Ramirez
3	Caída del canal de internet	Si la Falla es del Hardware y se puede solventar internamente se realiza el procedimiento correspondiente. • Verificación de los equipos de comunicación; tanto como el equipo de proveedor ISP y equipo de seguridad perimetral del MTPS • Se sustituye o se repara la parte con el Stock de	William Cerón Franklin Pineda Cesar Linares

#	RIESGOS	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO
		repuestos existentes. • Puesta en Operación del Equipo (Switches/router/AP). Si la Falla del Hardware es seria y no se puede solventar internamente se realiza lo siguiente: • Se comunica inmediatamente con el proveedor para hacer efectiva la garantía o se cumpla la clausula de remplazo de equipo • Si el equipo no tiene garantía, se debe realizar requerimiento de compra.	
4	Caída del Servicio Telefónico	Si la Falla es del Hardware y se puede solventar internamente se realiza el procedimiento correspondiente. • Verificación de los equipos de comunicación, y los enlaces El. • Se comunica inmediatamente con el proveedor para hacer efectiva la garantía del enlace. • Verificar si hay falla física en las tarjetas marca san goma, Sí el equipo no tiene garantía, se debe realizar requerimiento de compra. • Verificar cableado.	William Cerón Robin Medina Franklin Pineda
5	Caída de servicios por virus informático	• Verificar los servicios y detectar los que han sido afectados. • Aislar el servicio afectado • Escaneo de archivos con antivirus • Verificar si es una nueva variante de ransonware, para solicitar al proveedor de	William Ceron Franklin Pineda Blanca Ramírez Willian Rivera

#	RIESGOS	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO
		antivirus un parche para evitar la propagación del mismo. • Verificación y comprobación de la información encriptada y que fue recuperada Si el equipo afectado con virus es encriptado totalmente y no hay recuperación de la información. • Se verificaron los respaldos • Se recuperará la información.	
6	Suspensión del servicio por sismo, inundación o incendio	Verificar si hay acceso al centro de datos. si es así realizar apagado de los servidores. Se procederá a activar el sltio de contingencia	William Cerón Franklin Pineda Willian Rivera Blanca Ramírez Cesar Linares
7	Retrasos en el Proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad.	Verificar las fechas de vencimiento de los servicios a contratar Realizar el requerimiento del servicio con tiempo de anticipación Ver1f1cación del estado en el que se encuentra el proceso de compra	Administrador de contrato UACI
8	Pérdida de informadón considerada confidencial o de reserva por robo, alteración o extracción.	Si la perdida de información es de un equipo informático del centro de datos Se verificará a las personas que tienen acceso a esos recursos	Franklin Pineda William Ceron Blanca Ramírez

#	RIESGOS	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO
		Se verificará la cantidad de archivos del equipo alterado contra los respaldos de información dedicada.	
9	Falla técnica en equipos servidores, de escritorio o de comunicaciones.	Si la Falla es de Software y se puede solventar internamente se realiza el procedimiento siguiente: • Se repara, instala o desinstala el software según el caso • Se verifica la Configuración del servidor para la puesta en Operación. • Si se ha realizado un reinicio de Sistema Operativo, se restauran los respaldos correspondientes. • Puesta en marcha del servidor. Si la Falla es de Hardware y se puede solventar internamente se realiza el procedimlento siguiente • Se repara o sustituye la parte con el Stock de Repuestos existente. • Se verifica la Configuración del servidor para la Puesta en Operación. (Si se ha realizado un reinicio de Sistema Operativo a causa de la sustitución del hardware ya se parcial o total se restauran los respaldos correspondientes). • Puesta en Operación del Servido	Franklin Pineda Blanca Ramírez
10	Falla técnica en sistemas de información.	Si la Falla del Hardware se puede solventar internamente se realiza el Procedimiento correspondiente.	William Cerón Willian Rivera

#	RIESGOS	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO
		• se verifica que hardware está creando la falla en los sistemas • Se sustituye o repara el hardware que genera la falla. • Se verifica la configuración del equipo y/o servidor para la puesta en operación. • Sí la falla genero un restablecimiento de configuración o reinicio de fábrlca, se deben de restaurar todos sus componentes de configuración y/o datos a través de una copia de seguridad. • Puesta en Operación del Equipo y/o servidor correspondiente. Si la Falla del Software se puede solventar internamente se realiza el Procedimiento correspondiente: • Se repara, instala o desinstala el software según el caso • Se verifica la Configuración del servidor para la puesta en Operación. • Si se ha realizado un reinicio de Sistema Operativo, se restauran los respaldos correspondientes. • Puesta en marcha del servidor.	

CLASIFICACION DE INTERRUPCIONES Y NIVEL DE AFECTACION A LOS SERVICIOS DE TI

La activación o no del plan de Contingencias de TI del Ministerio de Trabajo y Previsión Social, dependerá de las decisiones tomadas por la jefatura de la Unidad de Desarrollo Tecnológico de este Plan de Contingencias de TI, frente a la situación que genere la interrupción del servicio tecnológico.

Los incidentes que pasan a ser tratados dentro del Plan de Contingencia de TI, son evaluados de acuerdo con el impacto que tienen sobre la prestación del servicio tecnológico del Ministerio de Trabajo y Previsión Social de acuerdo con la siguiente clasificación:

TIPO DE INTERRUPCIÓN	CARACTERfSTICAS	EJEMPLOS
TOTAL	Evento que inhabilita el centro de datos principal para prestar sus servicios. No permite que el equipo de tecnología continúe laborando en las instalaciones principales de la empresa.	!Terremotos. Incendio general. Orden Público. Fallo eléctrico en el sector.
PARCIAL	Evento que afecta a más de unrecurso informático de manera drástica ocasionando la suspensión parcial del funcionamiento del hardware o software considerados como críticos.	Fallas técnicas en equipos servidores que alojan más de un aplicativos, bases de datos.
ESPECIFICA	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática.	Fallas técnicas de un equipo que aloja un sistema o servicio Ausencia de personal clave.

La evaluación de la afectación de los servicios de TI, se definió con base en el impacto que puede generar la materialización de alguno de los riesgos identificados en el proceso de Gestión de Tecnologías de la Información en el desarrollo de las actividades propias de cada proceso, de la siguiente manera:

RECURSO AFECTADO	NIVEL DE AFECTACIÓN	TIEMPO DE RESPUESTA CONTINGENCIA
Servidores	Alto	48 horas
Sistemas de Información y/o aplicativos	Alto	48 horas
Servicio de Internet	Alto	4 horas
Correo Electrónico	Medio	3 horas
Página Web	Alto	24 horas
Red de datos	Alto	4 horas
Impresoras y escáneres	Bajo	4 horas
Corriente eléctrica	Alto	2 horas de respaldo de U PS CENTRALIZADO
Telefonía	Media	4 horas

RECOMENDACIONES

- Verificar periódicamente el directorio telefónico de contacto de los funcionarios responsables y mantenerlo actualizado.
- Verificar los procedimientos de copia y restauración de las copias de seguridad.
- Realizar jornadas de capacitación sobre et plan, a funcionarios de las diferentes áreas sobre las actividades a seguir en el proceso de contingencia.
- Solicitara los proveedores del servicio de Internet y correo electrónico el Plan de Contingencias que tienen definido para garantízar el servicio.

IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA DE TI

El plan aplica las actividades necesarias para mantener en operatividad los sistemas de información y/o aplicativos y la infraestructura tecnológica que los soporta, en el Ministerio de Trabajo y Previsión Soclal para su implementación es necesario tener en cuenta los aspectos técnicos, humanos y de logística descritos en este plan, que permitan estar preparados para afrontar cualquier contingencia.

CONTROL DE CAMBIOS

Descripción	Responsable	Fecha	Versión
Creación del Plan de Contingencia para la Continuidad de los Servicios Informáticos	Lic. Willlam Cerón Jefe Unidad de Desarrollo Tecnológico	5/02/2021	01