Consejo Universitario

RESOLUCIÓN DE CONSEJO UNIVERSITARIO
N°866 -2023-UNTRM/CU

Chachapoyas, 03 NOV 2023

VISTO:

El acuerdo de sesión ordinaria N° XI de Consejo Universitario, de fecha 02 de noviembre de 2023; y

CONSIDERANDO:

Que la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, organiza su Régimen de Gobierno de acuerdo a la Ley Universitaria N° 30220, su Estatuto y reglamentos, atendiendo a sus necesidades y características;

Que con Resolución de Asamblea Universitaria N° 001-2023-UNTRM/AU, de fecha 02 de enero de 2023, se aprueba el Estatuto de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, cuerpo normativo que consta de XXII Títulos, 178 Artículos, 04 Disposiciones Complementarias, 07 Disposiciones Transitorias, 01 Disposición Final, en 78 folios;

Que mediante Oficio N° 0156-2023-UNTRM-R-OTI, de fecha 24 de julio de 2023, el Director de la Dirección Tecnologías de la Información, remite a la Oficina de Planeamiento y Presupuesto la propuesta de *"Plan de Contingencia de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas"*, para su revisión y trámite correspondiente;

Que mediante Informe N° 157-2023-UNTRM-R-OPP/UM, de fecha 19 de octubre de 2023, el Jefe de la Unidad de Modernización, informa a la Jefa de la Oficina de Planeamiento y Presupuesto, que en virtud del principio de licitud y segregación de funciones, concluye: Que de la revisión del proyecto de plan presentado, se identifica que fue formulada en el marco de sus funciones, de modo que, contando previamente con el visto bueno del área usuaria, es factible la aprobación del proyecto de *"Plan de Contingencia de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas"*, en ese sentido, recomienda derivar los actuados que obran en el expediente administrativo a la Oficina de Asesoría Jurídica para el pronunciamiento legal que amerite;

Que con Oficio N° 1907-2023-UNTRM-R/OPP, de fecha 23 de octubre de 2023, la Jefa de la Oficina de Planeamiento y Presupuesto, remite a la Jefa de la Oficina de Asesoría Jurídica, el proyecto de *"Plan de Contingencia de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas"*, para el pronunciamiento legal que amerite, y posteriormente sea derivado a la Dirección General de Administración, para los trámites consiguientes para su aprobación;

Que mediante Oficio N° 774-2023-UNTRM-R/OAJ, de fecha 26 de octubre de 2023, la Jefa de la Oficina de Asesoría Jurídica, informa que en virtud a los documentos antes descrito, en los cuales previamente la Unidad de Modernización y la Oficina de Planeamiento y Presupuesto de esta Casa Superior de Estudios brindaron el visto bueno del proyecto de *"Plan de Contingencia de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas"*, en ese sentido hace de conocimiento lo siguiente: *Que respecto al extremo de la base legal contenido en la propuesta del referido Pla, se visualiza que estos se encuentran concordes al ordenamiento jurídico, de manera que esta oficina procede a brindar conformidad en dicho extremo y dar el visto bueno correspondiente*; por lo tanto se deriva a su despacho con el fin de que continúe con el trámite respectivo;

Consejo Universitario

RESOLUCIÓN DE CONSEJO UNIVERSITARIO
N° 866 -2023-UNTRM/CU

Que mediante Oficio N° 4671-2023-UNTRM-R/DGA, de fecha 30 de octubre de 2023, la Directora General de Administración, remite al señor Rector, el proyecto de *"Plan de Contingencia de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas"*, que encontrándose acorde al marco normativo y con el visto bueno de las áreas competentes, recomienda poner a consideración del Consejo Universitario para su respectiva aprobación;

Que asimismo, el Estatuto Universitario, prescribe en el *"Artículo 30. Consejo Universitario. El Consejo Universitario es el máximo órgano de gestión, dirección y ejecución académica y administrativa de la UNTRM. (...)"*;

Que el Consejo Universitario en sesión ordinaria, de fecha 02 de noviembre de 2023, acordó aprobar el *"Plan de Contingencia de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas"*, la cual consta en treinta y un (31) folios;

Que estando a lo expuesto y en ejercicio de las atribuciones que la Ley Universitaria N° 30220, el Estatuto Universitario y el Reglamento de Organización y Funciones aprobado mediante Resolución Rectoral N° 022-2023-UNTRM/R y ratificado con Resolución de Consejo Universitario N° 012-2023-UNTRM/CU, le confieren al Rector en calidad de Presidente del Consejo Universitario de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, y contando con los vistos buenos de la Dirección General de Administración, Oficina de Planeamiento y Presupuesto, Oficina de Asesoría Jurídica;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR el ***"Plan de Contingencia de Tecnologías de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas"***, que como anexo forma parte integrante de la presente resolución en treinta y un (31) folios.

ARTÍCULO SEGUNDO.- DEJAR SIN EFECTO las disposiciones internas que se opongan a la presente resolución.

ARTÍCULO TERCERO.- NOTIFICAR la presente resolución a los estamentos internos de la universidad, de forma y modo de Ley para conocimiento y fines.

REGÍSTRESE Y COMUNÍQUESE.

UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS
Jorge Luis Maicelo Quintana Ph.D.
Rector

UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS
Abg. Mag. Roger Angeles Sánchez
Secretario General

JLMQ/R.
RAS/SG
Crhm/.

UNIVERSIDAD NACIONAL
TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

ÍNDICE

INTRODUCCIÓN

La creciente demanda para acceder a servicios de Tecnologías de la Información (TI) de calidad por parte de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, acrecienta directamente proporcional al incremento exponencial de la comunidad universitaria, lo cual supone una afección en el servicio sin previo aviso. Considerando que la información es parte fundamental para la institución, de la misma manera los ambientes y recursos tecnológicos que la contienen representan activos valiosos, no obstante, estos se encuentran expuestos a distintas amenazas internas o externas que podrían perjudicar la confiabilidad, integridad y disponibilidad de los servicios TI, provocando la pérdida de información o deterioro de recursos tecnológicos por lo cual representaría un impacto económico y operativo negativo para la institución.

Para ello es necesario resguardar todo tipo de información ante cualquier alteración, supervisar el comportamiento y el mantenimiento continuo de los ambientes y recursos tecnológicos, significa la continuidad operativa de la infraestructura de tecnológica esto repercute en calidad de servicio. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible.

La Oficina de Tecnologías de la Información de la Universidad Toribio Rodríguez de Mendoza de Amazonas (OTI) presenta el *"Plan de Contingencia de Tecnologías de la Información de la Universidad Nacional Toribio Rodríguez de Mendoza - 2023"*, el cual contiene acciones o procedimientos alternativos que se deberá ejecutar ante una posible ocurrencia de eventos, ya sean de carácter técnico, humano, accidental o por desastres naturales.

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS

I. FINALIDAD

Establecer los procedimientos que garanticen la continuidad de las operaciones de tecnologías de la información en la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (UNTRM), estableciendo ciertas medidas técnicas y organizativas a fin de asegurar y restaurar los servicios en el menor tiempo posible, minimizando el impacto negativo en el caso de suscitarse una incidencia.

II. OBJETIVO GENERAL

Definir los procedimientos necesarios que deberán ser realizados ante determinados eventos que podrían alterar el normal funcionamiento, a fin de poder garantizar seguridad integridad y disponibilidad de la información y la continuidad operativa y disponibilidad de los servicios tecnológicos de la institución, para lo cual se establecen medidas técnicas y organizativas con el propósito de asegurar y restaurar los servicios en forma rápida, eficiente y oportuna, minimizando el impacto negativo sobre los mismos.

III. OBJETIVOS ESPECÍFICOS

- Identificar y analizar los posibles riesgos que pueden afectar las operaciones, procesos y servicios de TI.
- Contar con una estrategia documentada y actualizada que garantice la continuidad de las operaciones de los servicios de TI.
- Definir actividades de planeación, preparación, ejecución y retroalimentación para la mitigación del impacto y la recuperación de los servicios de TI ante un desastre, incidencia o evento.
- Prevenir y minimizar la pérdida o la corrupción de información digital; así como el daño permanente a los recursos tecnológicos que dan continuidad a los servicios.
- Proporcionar una respuesta inmediata y apropiada ante un incidente imprevisto, para un trabajo a corto plazo.

IV. BASE LEGAL

- Ley N° 27347, Ley de creación de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas.
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley N° 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia.

- Ley N° 27347, Ley de creación de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas.
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley N° 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia
- Decreto Supremo N° 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Resolución Ministerial N° 246-2006-PCM, que aprueba la Estrategia Nacional de Gobierno Electrónico.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP/ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de Buenas Prácticas para la gestión de la Seguridad de la información. 2da. Edición" en todas las entidades integrantes del Sistema Nacional.
- Resolución Ministerial N° 129-2012-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP/ISO/IEC 27001:2008 EDI Tecnología de la información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.
- Norma ISO 22301:2012. Seguridad de la Sociedad – Sistemas de Gestión de la Continuidad del Negocio – Requisitos.
- 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.
- 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.
- Resolución de Asamblea Universitaria N° 001-2023-UNTRM-AU, que aprueba el Estatuto de la UNTRM.
- Resolución Rectoral N° 022-2023-UNTRM/R, que aprueba el Reglamento de Organización y Funciones de la UNTRM.

V. ÁMBITO DE APLICACIÓN

Las disposiciones contenidas en el plan son de aplicación y cumplimiento obligatorio para todos los órganos y unidades orgánicas de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, consecuentemente, para todo el personal, independientemente de su régimen o vínculo laboral, que preste servicios en la UNTRM.

VI. ACRÓNIMOS Y DEFINICIONES O GLOSARIO DE TÉRMINOS

UNTRM	:	Universidad Toribio Rodríguez de Mendoza de Amazonas.
OTI	:	Oficina de Tecnologías de la Información.
TI	:	Tecnologías de la Información.
PEI	:	Plan Estratégico Institucional.

IP	:	Internet Protocol.
Ethernet	:	Tecnología para conectar dispositivos en una red LAN.
Storage	:	Almacenamiento.
Switch	:	Dispositivo de conexión en una red.
UPS	:	(Uninterruptable Power Supply) Sistema de alimentación Ininterrumpida.
SISNOA	:	Sistema de no adeudo.
SIAF	:	Sistema Integrado de Administración Financiera.
SIGA	:	Sistema Integrado de Administración financiera.
DAYRA	:	Dirección de Admisión y Registros Académicos.
VRIN	:	Vicerrectorado de Investigación.
SPSS	:	(Package for Social Sciences) Paquete Estadístico para Ciencias Sociales.
MBPS	:	Megabits por segundo.
PC	:	(Personal Computer) Computadora Personal.
Hardware	:	Componentes físicos que componen una computadora.
Software	:	Conjunto de programas, reglas órdenes que se ejecutan en una computadora.
Backup	:	Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

VII. ENFOQUE ESTRATÉGICO DE LA ENTIDAD

7.1 Misión de la UNTRM

"Formar profesionales líderes a través de una educación de calidad basada en investigación e innovación con sentido humanista, a estudiantes universitarios capaces de afrontar los retos de un entorno globalizado con ética, comprometidos con la diversidad cultural y el desarrollo sostenible de la sociedad"

7.2 Visión de la UNTRM

"Ser líder y referente nacional e internacional en formación académica, investigación científica, tecnológica y humanista de calidad que contribuya al desarrollo de la sociedad".

7.3 Plan Estratégico Institucional

El Plan Estratégico Institucional – PEI 2023- 2030, es un documento de planificación con visión y acciones estratégicas, para el cumplimiento de los objetivos instituciones, por lo cual la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas, implementa como parte de sus instrumentos de gestión el Plan de Contingencia de Tecnologías de la Información 2023, que se encuentra alineado a la acción estratégica institucional – AEI.05.02, Plan de gestión de riesgos de la Gestión Institucional implementado para la comunidad universitaria, que pertenece al

Objetivo Estratégico Institucional – OEI.05 "Implementar la gestión del riesgo de desastres".

7.4 Oficina de Tecnologías de la Información - OTI

La Oficina de Tecnologías de la Información, es el órgano de apoyo responsable de gestionar las Tecnologías de la Información de manera integral en todo el ámbito académico y administrativo de la UNTRM.

VIII. INFRAESTRUCTURA TECNOLÓGICA

8.1 Servidores informáticos

La Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas cuenta con un conjunto de 17 (diecisiete) servidores que se encuentran rackeados dentro de los gabinetes del Centro de Datos, ubicado en el edificio de la Oficina de Tecnologías de la Información, estos servidores dan soporte a los diferentes servicios y sistemas de información de la entidad.

8.2 Almacenamiento informático

Con la finalidad de asegurar la integridad, confiabilidad y disponibilidad de la información la UNTRM cuenta con dispositivos y sistemas de almacenamiento en el centro de datos con una capacidad de 80 Terabyte's de almacenamiento.

8.3 Conmutador de acceso

Actualmente la institución cuenta con 79 conmutadores de acceso, equipos que permiten la interconexión de múltiples dispositivos dentro de una misma red los cuales están distribuidos en la sede administrativa y en los diferentes pabellones de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas.

8.4 Sistema de Protección Eléctrica

Un sistema de protección se utiliza para proteger y evitar posibles errores o destrucciones de instalaciones o perdidas de equipos. Estos aíslan la zona donde se ha originado el fallo con el fin de evitar la expansión del error y la aparición de consecuencias más graves, el centro de datos ubicado en la Oficina de Tecnologías de la Información cuenta con los siguientes sistemas de protección eléctrica:

- Sistema de Aislamiento
- UPS (Sistemas de alimentación ininterrumpida)
- Pozo a tierra
- Para rayos
- Generador eléctrico
- Transformador eléctrico.

8.5 Servicios brindados por el centro de datos de la OTI

El Centro de Datos ubicado en el edificio de la Oficina de Tecnologías de la Información de la UNTRM, brinda servicios en Tecnologías de la Información a la comunidad universitaria, a través de los diferentes sistemas informáticos; entre estos se encuentran: El Sistema de Gestión Académica, Sistema de no Adeudo (SISNOA), Sistema Integrado de Administración Financiera (SIAF), Sistema Integrado de Gestión Administrativa (SIGA), Sistema de Tesorería, Sistema de Admisión y el Sistema de Recursos Humanos.

Además, el Centro de Datos de la OTI, brinda el servicio de redes e internet (ethernet y wifi) y servicio de telefonía IP, esta tecnología permite realizar y recibir llamadas de voz a través de internet dentro del campus universitario.

8.6 Licencias de Software

La adquisición de licencias de software garantiza el correcto funcionamiento de los programas informáticos sin ninguna anomalía, permitiendo que los usuarios accedan a características adicionales, los mismos estarán actualizadas y con soporte directo del fabricante, además evitan futuras penalidades que se ocasionen a la Universidad Nacional Toribio Rodríguez de Mendoza, en este sentido nuestra institución cuenta con las siguientes cantidades de licencias de sistemas:

N°	SISTEMA	CANTIDAD DE LICENCIAS
01	Microsoft Office Professional	110
02	Microsoft SQL Server Standard	16 x 8
03	Windows Remote Desktop	50
04	Microsoft SQL Server CAL	110
05	Windows Server Data Center	32 x 8
06	Windows Server Standard	32 x8
07	Microsoft Windows Pro	110
08	SPSS	21
09	Antivirus Kaspersky	600

Tabla 1: Licencias de Software.

8.7 Sistemas de Información

Con la finalidad de ayudar a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales de la institución, cuenta con los siguientes sistemas de información:

N°	NOMBRE	SIGLAS	DESCRIPCIÓN	ÁREA RESPONSABLE
01	Sistema Integrado Académico	SIA	Permite la gestión académica.	DAYRA
02	Sistema Integrado de Gestión Administrativa	SIGA	Simplifica y automatiza los procesos administrativos de la entidad.	Todas las áreas administrativas
03	Sistema Integrado de Gestión Financiera	SIAF	Permite el registro único y obligatorio de toda la información financiera de la entidad.	Dirección General de Administración y Oficina de Planeamiento Estratégico y Presupuesto
04	Sistema de no Adeudo	SISNOA	Registra el estado de deuda de la comunidad universitaria.	VRIN
05	Sistema de Tesorería	Sistema de Tesorería	Registra ingresos de recursos económicos.	Unidad de Tesorería
06	Sistema de Admisión	Sistema de Admisión.	Registra: Inscripción de postulantes, control de aula y generación de constancia de ingreso de postulantes.	DAYRA
07	Sistema de Recursos Humanos	Sistema de Recursos Humanos	Registra información del recurso humano de la entidad (Planilla de remuneraciones, control de asistencia, Legajo y archivo).	Recursos Humanos

Tabla 2: Sistemas de Información

8.8 Equipos de Cómputo

La UNTRM cuenta con la siguiente cantidad de equipos:

EQUIPO	CANTIDAD
Servidor	17
Computador de escritorio	744
Computador portátil	84

Tabla 3: Equipo de Cómputo

8.9 Equipos de Impresión

La UNTRM cuenta con la siguiente cantidad de equipos:

EQUIPO	CANTIDAD
Impresora	115

Tabla 4: Equipos de Impresión

8.10 Equipos de Redes y Conectividad

La UNTRM cuenta con la siguiente cantidad de equipos:

EQUIPO	CANTIDAD
Switch	79
Punto de Acceso	105

Tabla 5: Equipos de Redes y Conectividad

8.11 Equipos de Audio y Video

La UNTRM cuenta con la siguiente cantidad de equipos:

EQUIPO	CANTIDAD
Proyector	160
Cámara de Vigilancia	72
Cámara Fotográfica	15

Tabla 6: Equipo de redes y conectividad.

8.12 Conectividad a Internet

La sede de la UNTRM cuenta actualmente con conexión a internet de línea dedicada de 500 MBPS de velocidad. La filial Bagua cuenta con conexión de fibra óptica de 40 MBPS y la filial Utcubamba cuenta con una conexión a internet de 30 MBPS de velocidad cada una.

IX. PLAN DE CONTINGENCIA DE LOS SERVICIOS INFORMÁTICOS DE LA UNTRM

9.1 METODOLOGÍA

La metodología está elaborada en fases, las cuales son:

- Identificación de Riesgos.
- Estrategias para la recuperación de desastre, incidencia o evento.
- Realización de pruebas (Implementación).

Las escalas a utilizar en el presente documento corresponden a:

9.1.1 Escala Cualitativa de Probabilidad

Son escalas descriptivas para demostrar la magnitud de consecuencias potenciales y su posibilidad de ocurrencia. Para cada riesgo identificado se evalúan los niveles de probabilidad de impacto.

CATEGORÍA	DEFINICIÓN
ALTO	Es muy probable la materialización del riesgo o se presume que llegará a materializarse.
MEDIO	Es probable la materialización del riesgo o se presume que llegará a materializarse.
BAJO	Es poco probable la materialización del riesgo o se presume que llegará a materializarse.

Tabla 7: Escala Cualitativa de Probabilidad

9.1.2 Escala Cuantitativa de Impacto

Se usa el mismo diseño que fue definido para la escala cualitativa, la escala cuantitativa se detalla a continuación:

CATEGORÍA	DEFINICIÓN
ALTO	Si el hecho llegara a presentarse, se tendría alto impacto o efecto sobre la entidad.
MEDIO	Si el hecho llegara a presentarse, se tendría medio impacto o efecto sobre la entidad.
BAJO	Si el hecho llegara a presentarse, se tendría bajo impacto o efecto sobre la entidad.

Tabla 8: Escala Cualitativa de Probabilidad

9.1.3 Escalas Cuantitativas de Probabilidad e Impacto

Se muestra las escalas cuantitativas de probabilidad de impacto.

PROBABILIDAD DE OCURRENCIA	NIVEL
1	Bajo
2	Medio
3	Alto

Tabla 9: Escala cuantitativa de Probabilidad.

IMPACTO	NIVEL
1	Bajo
2	Medio
3	Alto

Tabla 10: Escalas cuantitativas de probabilidad e impacto

9.1.4 Evaluación y Clasificación del Riesgo

Evaluación y Clasificación del Riesgo			PROBABILIDAD		
			BAJO	MEDIO	ALTO
			1	2	3
IMPACTO	ALTO	3	(3) Riesgo Moderado	(6) Riesgo Importante	(9) Riesgo Inaceptable
	MEDIO	2	(2) Riesgo Tolerable	(4) Riesgo Moderado	(6) Riesgo Importante
	BAJO	1	(1) Riesgo Aceptable	(2) Riesgo Tolerable	(3) Riesgo Moderado

Tabla 11: Evaluación y Clasificación del riesgo

9.1.5 Niveles de Riesgo

NIVEL DE RIESGO: CUALITATIVO	NIVEL DE RIESGO: CUANTITATIVO	PRIORIDAD	DESCRIPCIÓN
Riesgo Inaceptable	9	MUY ALTA	Se requiere de una acción inmediata, planes de tratamientos necesarios, implementados y reportados a la alta dirección.
Riesgo Importante	6	ALTA	Se requiere planes de tratamiento necesarios, implementados y reportados a los jefes de las oficinas, direcciones entre otros.
Riesgo Moderado	4 y 3	MEDIA	Debe ser administrado con procedimientos normales de control.
Riesgo Tolerable	2	BAJA	Menores efectos que pueden ser fácilmente remediados, se administran con procedimientos rutinarios.
Riesgo Aceptable	1	MUY BAJA	Riesgo insignificante. No se requiere ninguna acción.

Tabla 12: Niveles de Riesgo

9.1.6 Cuantificación de los Riesgos

Los riesgos son cuantificados de acuerdo a dos factores:

- PROBABILIDAD: representa la posibilidad de que se presente el desastre, incidencia o evento.
- IMPACTO: representa la importancia del riesgo, es decir cuánto puede afectar.

RIESGO = PROBABILIDAD x IMPACTO

9.2 IDENTIFICACIÓN DE RIESGOS

9.2.1 Análisis de Riesgos

La UNTRM se encuentra expuesta a ciertos riesgos que pueden ser causados por eventos imprevistos o por el mal uso de los recursos, haciendo que afecte a los objetivos o metas de la entidad. Por lo que, la identificación de riesgos está relacionado a aquellos que afectan la seguridad del centro de datos y la infraestructura tecnológica, que trae como consecuencia la indisponibilidad, operación y continuidad de los servicios informáticos.

9.2.2 Relación de los Riesgos que pueden afectar al Centro de Datos

A continuación, son detallados los riesgos identificados:

Nro	Riesgo Identificado	Descripción del Riesgo	Consecuencia
01	Terremoto	Fenómeno natural manifestado por una sacudida brusca de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas sísmicas.	Destrucción del ambiente destinado para el centro de datos y/o gabinetes de comunicación de la Intranet, generando la interrupción de todos los servicios que brindan.
02	Inundación	Ocupación de agua en zonas que habitualmente están libres debido a lluvias torrenciales o ruptura de sistema de agua potable.	Deterioro de equipos por el ingreso de agua al ambiente del centro de datos, canalizaciones subterráneas de comunicación de datos y gabinetes de comunicación de la Intranet en las diferentes sedes de la UNTRM; generando la interrupción de todos los servicios que brinda.
03	Tormenta eléctrica	Una tormenta local producida por una nube cumulonimbos y que está acompañada por relámpagos y truenos" La caída de un rayo dentro de un radio de 8 a 16 kilómetros generan un valor mayor a 2000V/m.	Deterioro de equipos por descarga eléctrica (Rayo). Generando la interrupción de todos los servicios que brindan los equipos activos de la infraestructura de red.
04	Incendio	Ocurrencia de fuego no controlado.	Destrucción de los ambientes y equipos destinados para el centro de datos y/o gabinetes de comunicación de la Intranet, generando la interrupción de todos los servicios que brindan.
05	Vandalismo	Actitud o inclinación a cometer acciones destructivas contra la propiedad pública sin consideración alguna hacia los demás.	Interrupción parcial o total de los servicios que brindan el centro de datos y los equipos de la infraestructura de red.
06	Fraude	Evento referido a la alteración de datos para uso en contra de la institución o en beneficio del autor del acto.	Uso ilícito de los recursos de la UNTRM en contra de la institución.
07	Intrusión de la red de datos	Ataque que provienen localmente o de internet, originados por intrusos, virus, malware, etc., con la finalidad de alterar el normal funcionamiento de los recursos informáticos.	Interrupción parcial o total de los servicios que brindan el centro de datos y equipos de la infraestructura de red de la intranet.
08	Interrupción del fluido eléctrico	Pérdida del suministro eléctrico en el centro de datos o gabinetes de comunicación de la Intranet.	Posibles daños en los equipos sensibles o pérdida de información originando una interrupción en los servicios que brindan.

Tabla 13: Riesgos comunes que podrían afectar al centro de cómputo y/o intranet

9.2.3 Cuantificación de los Riesgos Identificados

En el siguiente cuadro se detallan la clasificación de los riesgos identificados, la cual es evaluada de acuerdo al juicio de expertos.

MATRIZ DE PROBABILIDAD POR IMPACTO					
N°	**Riesgo Identificado**	**Probabilidad (P)**	**Impacto (I)**	**(P) x (I)**	**Nivel de Riesgo**
01	Terremoto	2	3	6	Riesgo Importante
02	Inundación/ Aniego	1	4	4	Riesgo Moderado
03	Tormenta eléctrica	1	4	4	Riesgo Moderado
04	Incendio	1	3	3	Riesgo Moderado
05	Vandalismo	1	2	2	Riesgo Bajo
06	Fraude	1	2	2	Riesgo Bajo
07	Intrusión de la red de datos	2	2	4	Riesgo Moderado
08	Interrupción del fluido eléctrico	2	3	6	Riesgo Importante

Tabla 14: Cuantificación de Riesgos (Probabilidad por Impacto)

De la valoración realizada en la matriz de probabilidad por impacto, se ha identificado que existen riesgos cuyo nivel han sido valorados como importante y moderado según la probabilidad y el impacto que estos podrían generar en el centro de datos e Intranet de producirse.

En este sentido, concluimos que el análisis evidencia las posibles contingencias que pudieran presentarse y afectar a los sistemas de información y la plataforma que permite su operación, para lo cual el presente "Plan de Contingencia" desarrollará las estrategias a fin de poder mitigar los riesgos importantes y riesgos moderados identificados.

9.3 ESTRATEGIAS PARA LA RECUPERACIÓN ANTE DESASTRES

El uso de los medios electrónicos e informáticos genera beneficios, pero también riesgos asociados ante la ocurrencia de un desastre, incidente o evento por lo que se debe mitigar su impacto con acciones que permitan dar continuidad de los servicios de TI, por lo que son definidas acciones preventivas (antes), de ejecución (durante) y de recuperación (después).

9.3.1 Actividades Preventivas (antes)

Son aquellas actividades de planeamiento, preparación entrenamiento y ejecución de las acciones de resguardo de información que nos permita un proceso de recuperación viable de los servicios de TI proporcionados por el Centro de Datos y la infraestructura de red de la Intranet de la UNTRM. En ese sentido, se hace necesario el contar con la siguiente información:

Sistemas de información

La OTI debe contar con una relación de los Sistemas de Información; considerando lo siguiente:

- Nombre de la aplicación o Sistema.
- Lenguaje con el que fue creado el Sistema, incluyendo las librerías que lo conforman.
- Área usuaria, esto es la(s) dependencia(s) dueña del proceso sistematizado.
- Las unidades orgánicas que usan la información del sistema.
- El volumen de los archivos (en MB o GB) que trabaja el Sistema, si fuera el caso.
- El tamaño de las bases de datos (en MB o GB).
- El volumen de transacciones mensuales que maneje el sistema.
- Las fechas críticas, en las que la información es necesaria y debe estar disponible (la fecha en la que determinada información se está procesando)

Con esta información deberá realizarse una lista priorizada de los sistemas de información necesarios para que la UNTRM recupere la operatividad interrumpida en el desastre, incidente o evento (contingencia).

a. Hardware del centro de datos

La OTI, deberán señalizar o etiquetar los servidores, almacenamientos, equipos de infraestructura de red, cableado estructurado y PC's de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo, etiquetar de color rojo a los Servidores y Almacenamientos, color amarillo a las PC's con información importante o estratégica, color verde a los equipos de comunicación vitales para la conectividad. Alta disponibilidad de Hardware del centro de datos. Pudiendo ser implementado mediante dos modalidades:

- Modalidad Externa. Mediante convenio con otra Institución que tenga equipos similares o mayores (puede considerarse servicio en la nube) y que brinde la seguridad de poder procesar la Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido.
- Modalidad Interna. Contando con un centro de datos alterno, en ambos debemos tener identificado los equipos que, por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local.

En ambos casos se probará y asegurará que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los sistemas (continuidad)..

b. Respaldos de Información (backups)

Establecer los procedimientos (políticas o procedimientos de backup determinando responsabilidades en la obtención de los Backups críticos identificados) para la obtención de copias de seguridad necesarios para asegurar la disponibilidad de la información para la correcta ejecución de los sistemas o aplicativos ante la ocurrencia de un desastre, incidente o evento tales como:

N°	DESCRIPCIÓN
01	Archivos de configuración de aplicativos.
02	Código fuente de aplicativos.
03	Documentos adjuntos de aplicativos.
04	Archivos de unidades compartidas.
05	Motor de base de datos.
06	Software base de PC (OS, Browser, Ofimática, etc.).
07	Software base de servidores (OS, PHP, Java, etc.)

Tabla 15: Respaldo de Información

c. Hardware de la Infraestructura de Red

La OTI deberá identificar y etiquetar los equipos de infraestructura de red de la Intranet y cableado estructurado, de acuerdo a su importancia del servicio de conectividad que brinda, para ser priorizados en caso de una contingencia o evento, para ello es necesario tener en cuenta:

- Mantener un backup de los archivos de configuración de los equipos de infraestructura de red.
- Contar con el material y herramientas necesarias para el restablecimiento de la conectividad.

9.3.2 Actividades de Ejecución (durante)

Una vez presentada la contingencia, es necesaria la participación de todas las personas del área donde ocurre la contingencia para lo cual se debe:

- Identificar las vías de salida o escape.
- Realizar la evacuación de Personal.
- De ser factible, se debe colocar a buen recaudo los activos (incluyendo los activos de información).
- Identificar la ubicación y señalización de los elementos contra el siniestro (extintores de fuego, grifos de agua, etc.).
- Se debe seguir lo señalado en las fichas de contingencia para los casos identificados en el presente plan de contingencia (anexo 3).

a. Formación de equipo operativo

Deberán existir dos (02) equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos informáticos, de acuerdo a los lineamientos o clasificación de prioridades identificados para tal fin.

9.3.3 Actividades de Recuperación (después)

Inmediatamente después de que el desastre, incidente o evento ha concluido, se evaluará la magnitud de los daños producidos, estableciendo qué sistemas están afectados, qué equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo de acuerdo a la matriz de probabilidad por impacto. Luego de la evaluación, se identificarán las actividades a ser desarrolladas a fin de restaurar los servicios de TI afectados para lo cual se deberá tomar como referencia las actividades descritas en las fichas de contingencia identificadas (anexo 3).

a. Priorización de Actividades

Una vez efectuada la evaluación de daños, se deberá elaborar una lista de actividades que se deben realizar, priorizando en vista a las actividades estratégicas y urgentes de la UNTRM. El personal de la OTI cuyas actividades no se vieron afectadas se deberá asignar temporalmente para la solución de aquellas afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

b. Ejecución de Actividades

Las actividades identificadas y priorizadas para la recuperación de ocurrido el desastre, incidente o evento, deberán ser realizadas por los equipos de trabajo y se contará con un (01) coordinador que reportará el avance de los trabajos de recuperación a la jefatura a cargo del Plan de Contingencia y al Oficial de Seguridad de la Información. Los colaboradores que realizarán las actividades de recuperación tendrán dos etapas:

- La restauración de los servicios priorizados de TI del Centro de Datos.
- La restauración de todos los servicios priorizados de TI del Centro de Datos.

c. Evaluación de Resultados

Una vez concluidas las labores de recuperación del(los) sistema(s) que fueron afectados por el desastre, incidente o evento, se evaluará objetivamente todas las actividades, ¿qué tan bien se hicieron?, ¿qué tiempo tomaron?, ¿qué circunstancias modificaron?, ¿aceleraron o

entorpecieron las actividades del plan de acción?, ¿cómo se comportaron los equipos de trabajo?, etc.

De la evaluación de resultados y del siniestro, resultarán dos tipos de recomendaciones, la retroalimentación del Plan de Contingencias y una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el desastre, incidente o evento.

Con la evaluación de resultados, se optimizará el plan de contingencia original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que no funcionaron adecuadamente descritas en las fichas de contingencia.

9.4 REALIZACIÓN DE PRUEBAS (IMPLEMENTACIÓN)

9.4.1 Formación de Equipos Operativos para la Realización de Pruebas

El equipo operativo estará conformado por los colaboradores de la OTI, esto con la finalidad de realizar las pruebas antes de ocurrir un desastre, incidente o evento. Las actividades que serán realizadas corresponden a:

- Supervisar los procedimientos de respaldo y restauración de los sistemas de información.
- Participar en las pruebas y simulacros de desastres.
- Contar con un listado de personas que serán contactadas de ocurrir un desastre (anexo 2).

X. DISPOSICIONES FINALES

10.1 El Plan de Contingencias de TI deberá contar con el apoyo correspondiente por parte de la Alta Dirección, para suministrar de recursos financieros y humanos a fin de su implementación y ejecución.

10.2 La implementación y supervisión del Plan de Contingencia estará a cargo de un Comité, el cual garantiza la legalidad, consistencia, adecuado uso, seguridad, inviolabilidad y sostenibilidad de los Sistemas de Información, hardware y software.

10.3 La actualización del presente plan de contingencia debe ser realizada una vez al año.

10.4 Se deberá informar sobre las medidas adoptadas a todo el personal correspondiente debido a las amenazas latentes existentes.

XI. ANEXOS

ANEXO 01: Relación de sistemas de información.

ANEXO 02: Coordinación equipo de respuesta a emergencia en el centro de datos e intranet.

ANEXO 03: PROCESO: Gestión de Centro de Datos

ANEXO 01.
Relación de sistemas de información

ID	Nombre de la Aplicación
SI01	Sistema Integrado Académico (SIA)
SI02	Sistema Integrado de Gestión Administrativa (SIGA)
SI03	Sistema Integrado de Gestión Financiera (SIAF)
SI04	Sistema de no Adeudo (SISNOA)
SI05	Sistema de Tesorería
SI06	Sistema de Admisión
SI07	Sistema de Recursos Humanos

ANEXO 02.

Coordinación equipo de respuesta a emergencia en el centro de datos e intranet.

EQUIPO OPERATIVO		
N°	**CARGO**	**LUGAR DE TRABAJO**
01	Jefe de la Oficina de Tecnologías de la Información	OTI
02	Operador PAD	OTI
03	Técnico en Redes y Conectividad	OTI

ANEXO 03.

PROCESO: Gestión de Centro de Datos	**Código: 001**
Riesgo: INTRUSIÓN	

1. DESCRIPCIÓN DEL EVENTO

Ataques que provienen desde Internet, originados por hackers, virus con la finalidad de alterar el normal funcionamiento de los recursos informáticos, malware, etc.

1.1. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	**RESPONSABLE**			
	OTI	OTI	OTI	RECTOR
Actividades preventivas (antes)	C: Consultado	E: Encargado	R: Responsable	I: Informado

- Contar con respaldos actualizados des los datos electrónicos de la UNTRM, almacenados fuera del inmueble y/o en un servidor remoto.
- Contar con los equipos de seguridad perimetral actualizados y con soporte vigente.
- Contar con antivirus instalados en las PC´s y Servidores, actualizados y con soporte vigente.
- Verificar si se realizan respaldos de la información de manera periódica por la SODS y SORT, debiendo generar la respectiva acta de evidencia.
- Verificar si cuenta con actualización y soporte vigente de Firewall- NG y antivirus, debiendo generar la respectiva acta de evidencia.

1.2. ACTIVIDADES DE EJECUCIÓN (DURANTE)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	**RESPONSABLE**			
	OTI	OTI	OTI	RECTOR
Actividades de ejecución (durante)	I: Informado C: Consultado	E: Encargado	C: Consultado R: Responsable	I: Informado

- Confirmada la presencia de una intrusión en la red, se deberá investigar su origen para lo cual se de comprobar cuáles son los equipos y servicios que están siendo comprometidos a fin de identificar los causantes del ataque.
- Visualizar los procesos activos en los servidores a fin de identificar un comportamiento inusual en estos, debiendo considerar:
  - Procesos que llevan activos un largo periodo de tiempo.
  - Procesos que consumen un nivel elevado de CPU.
  - Procesos que no están ejecutados desde una PC perteneciente a la INTRANET de la UNTRM.
- Revisar los archivos de registro (log) a fin de obtener información sobre conexiones a lugares poco frecuentes, utilización de aplicaciones inusuales y otras actividades sospechosas de intrusión
- Chequeo de los archivos binarios del sistema a fin de detectar si han sido modificados.
- Comprobar los puertos de conexión abiertos; para detectar si hay alguno en especial que no lo debería ser.

- Analizar los directorios FTP/ HTTP/HTTPS/SMB a fin de detectar si alguno de ellos ha podido ser escrito por usuarios anónimos.
- Realizar el monitoreo del incidente.

1.3. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	RECTOR
Actividades de recuperación (después)	I: Informado	E: Encargado	C: Consultado R: Responsable	I: Informado C: Consultado

- De detectarse que la incidencia ha efectuado a algún componente de software o hardware del servidor, se debe comunicar al dueño de la información a fin de que verifique su impacto.
- Realizar un análisis forense de la intrusión en la red a fin de diseñar nuevas medidas que eviten incidentes futuros o parecidos.
- Si se comprueba que los equipos de seguridad han fallado en la detección de intrusos, debe recurrirse al proveedor a fin de comunicar el hecho.
- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución, debiendo llevar un control del mismo e informar al RECTOR.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

PROCESO: Gestión de Centro de Datos	**Código: 002**

Riesgo: TERREMOTO

1. DESCRIPCIÓN DEL EVENTO

Fenómeno natural manifestado por una sacudida brusca de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas sísmicas.

1.1. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	**RESPONSABLE**			
	OTI	OTI	OTI	OTI
Actividades preventivas (antes)	I: Informado	E: Encargado	R: Responsable	E: Encargado C: Consultado

- Revisar una vez al año la infraestructura donde se encuentra el centro de datos.
- Contar con respaldos actualizados de los datos electrónicos de la UNTRM, almacenados fuera del inmueble y/o en un servidor remoto.
- Asegurar que los elementos que se encuentren en el centro de datos sean ubicados de manera tal que permanezcan estables durante la contingencia y cumplan con el estándar para centro de datos.
- Se mantendrán cerradas las puertas de los gabinetes a fin de minimizar la caída de equipos u otros.
- Verificar la ejecución de las pruebas realizadas por la OTI, debiendo generar la respectiva acta de evidencia.
- Verificar si se realizan respaldos de la información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.

1.2. ACTIVIDADES DE EJECUCIÓN (DURANTE)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	**RESPONSABLE**			
	OTI	OTI	OTI	OTI
Actividades de ejecución (durante)	R: Responsable I: Informado	E: Encargado	I: Informado	E: Encargado C: Consultado

- Evacuar el área si es necesario, utilizando las rutas de emergencia buscando un lugar seguro y evitando ventanas, así como el uso de escaleras.
- Coordinar con la OTI para el corte del fluido eléctrico.
- Si el evento sucede en horario fuera de horas de trabajo, el personal de vigilancia de la UNTRM comunicará lo sucedido a la OTI.

1.3. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	**RESPONSABLE**			
	OTI	OTI	OTI	OTI
Actividades de recuperación (después)	I: Informado	E: Encargado	R: Responsable	C: Consultado

- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
- No ingresar al área afectada hasta que los expertos indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
- Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.
- Ante la posibilidad de un incendio, a solicitud de la OTI realizar el corte de fluido eléctrico y/o cerrar el paso de agua aledañas al centro de datos.
- Brindar el apoyo necesario a la OTI para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.
- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución, debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de Contingencia (mejora continua) y actualizar las fichas de contingencia.

PROCESO: Gestión de Centro de Datos	Código: 003

Riesgo: INUNDACIÓN / ANIEGO

1. DESCRIPCIÓN DEL EVENTO

Ocupación de agua en zonas que habitualmente están libres debido al desbordamiento de ríos, torrenteras, lluvias torrenciales, canales de regadío, entre otros.

1.1. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	OTI
Actividades preventivas (antes)	I: informado	I: Informado	R: Responsable	E: Encargado C: Consultado

- Revisar una vez al año el espacio físico donde se encuentra el centro de datos para descartar la existencia de filtraciones de agua.
- Revisar una vez al año los sistemas de desagüe y drenaje en el área circundante al centro de datos.
- Contratar una vez al año la revisión y mantenimiento de las alarmas de inundación o aniego.
- Señalizar las llaves de paso de agua al centro de datos.
- Contar con respaldos actualizados de los datos electrónicos de la UNTRM, almacenados fuera del inmueble y/o en un servidor remoto.
- Verificar que los cables del cableado estructurado no se encuentren expuestos a posibles inundaciones o aniegos.
- Verificar la ejecución de las pruebas realizadas por la OTI, debiendo generar la respectiva acta de evidencia.
- Verificar si se realizan respaldos de la información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.

1.2. ACTIVIDADES DE EJECUCIÓN (DURANTE)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	OTI
Actividades de ejecución (durante)	R: Responsable I: Informado	E: Encargado	I: Informado	E: Encargado C: Consultado

- Evacuar el área, utilizando las rutas de emergencia de ser el caso.
- Únicamente si los expertos indican que es seguro, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado, de ser factible.
- Coordinar con la OTI el corte de fluido eléctrico.
- Realizar el corte de fluido eléctrico a solicitud de la OTI.
- Si el agua proviene del interior cerrar las llaves de paso que sean necesarias.
- Si el agua proviene del exterior, cerrar las llaves de paso que sean necesarias y bloquear las entradas de agua.
- Si el evento sucede en horario fuera de horas de trabajo, el personal de vigilancia de la UNTRM comunicará lo sucedido a la OTI.

1.3. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	OTI
Actividades de recuperación (después)	I: Informado	E: Encargado	R: Responsable	C: Consultado

- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
- No ingresar al área afectada hasta que los expertos indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
- Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.
- Realizar las coordinaciones necesarias para extraer el agua y/o humedad de las zonas afectadas.
- Brindar el apoyo necesario a la OTI para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.
- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución, debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de Contingencia (mejora continua) y actualizar las fichas de contingencia.

PROCESO: Gestión de Centro de Datos	**Código: 004**

Riesgo: INCENDIO

1. DESCRIPCIÓN DEL EVENTO

Ocurrencia de fuego no controlado que puede afectar a los bienes.

1.1. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	**RESPONSABLE**			
	OTI	OTI	OTI	OTI
Actividades preventivas (antes)	I: Informado	E: Encargado	R: Responsable	E: Encargado C: Consultado

- Programar una vez al año la revisión y mantenimiento de alarmas contra incendios.
- Programar una vez al año la recarga de extintores y la capacitación del personal en el uso de los mismos.
- Contar con respaldos actualizados de los datos electrónicos de la UNTRM, almacenados fuera del inmueble y/o en un servidor remoto.
- Verificar que los cables del cableado estructurado no se encuentren cerca a posibles fuentes de calor.
- Verificar una vez al año que el cableado eléctrico y tomas eléctricas se encuentren en condiciones óptimas de operación.
- Verificar la ejecución de las pruebas realizadas por la OTI, debiendo generar la respectiva acta de evidencia.
- Verificar si se realizan respaldos de la información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.
- Verificar la ejecución de las pruebas realizadas por las SOST y SORT, debiendo generar la respectiva acata de evidencia.

1.2. ACTIVIDADES DE EJECUCIÓN (DURANTE)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	**RESPONSABLE**			
	OTI	OTI	OTI	OTI
Actividades de ejecución (durante)	R: Responsable	E: Encargado	I: Informado	C: Consultado

- Evacuar el área, utilizando las rutas de emergencia de ser el caso.
- Alertar a los bomberos, para ello se recurrirá a los números telefónicos de emergencia, a efectos de obtener una pronta respuesta al acontecimiento.
- Únicamente si los expertos indican que es seguro, desconectar los equipos de comunicaciones, servidores y sistemas de almacenamiento del centro de datos considerando su correcto apagado de ser factible.
- Coordinar con la OTI para el corte del fluido eléctrico.
- Realizar el corte de fluido eléctrico a solicitud de la OTI.
- Si el evento sucede en horario fuera de horas de trabajo, el personal de vigilancia de la UNTRM comunicará lo sucedido a la OTI.

1.3. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	OTI
Actividades de recuperación (después)	I: Informado	E: Encargado	R: Responsable	C: Consultado

- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
- No ingresar al área afectada hasta que los expertos indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
- Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.
- Brindar el apoyo necesario a la OTI para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.
- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución, debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de Contingencia (mejora continua) y actualizar las fichas de contingencia.

PROCESO: Gestión de Centro de Datos	Código: 005

Riesgo: TORMENTA ELÉCTRICA

1. DESCRIPCIÓN DEL EVENTO

Situación de atención que se declara bajo determinadas condiciones climáticas que podrían generar descargas eléctricas atmosféricas. Se definen tres niveles de alerta:

- Alerta Amarilla: Es una alerta preventiva que indica una actividad de tormenta eléctrica (caída de rayo) en un radio comprendido entre 16 a 30 kilómetros de distancia, tomando como centro de referencia la ubicación del centro de datos.
- Alerta Naranja: Es una alerta de advertencia que indica una actividad de tormenta eléctrica que se podría dar en dos casos:
  - Caída de rayo dentro del radio de 8 a 16 kilómetros de distancia, tomando como referencia la ubicación del centro de datos.
  - Caída de rayo dentro del radio de 16 a30 kilómetros y adicionalmente se registran un valor mayor a 2000 V/m.
- Alerta Roja: Es una alerta de peligro que indica una actividad de tormenta eléctrica que se podría dar en dos casos:
  - Caída de rayo dentro del radio de 0 a 8 kilómetros, tomando como centro de referencia la ubicación del centro de datos.
  - Caída de un rayo dentro de un radio de 8 a 16 kilómetros y adicionalmente se registran un valor mayor a 2000 V/m.

1.1. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	OTI
Actividades preventivas (antes)	I: Informado	I: Informado	R: Responsable	E: Encargado C: Consultado

- Asegurar que todas las instalaciones contra tormentas eléctricas estén identificados y adecuadamente señalizados.
- Asegurar que todo el personal este adecuadamente entrenados.
- Asegurar que los contratistas que trabajen cumplan o excedan con lo indicado en el presente estándar.
- Contar con respaldos actualizados de los datos electrónicos de la UNTRM, almacenados fuera del inmueble y/o en un servidor remoto.
- Verificar que los cables del cableado estructurado no se encuentren en malas condiciones.
- Realizar la coordinación con las áreas involucradas para realizar las pruebas de inspección de las alarmas sonoras y visuales.
- Verificar la ejecución de las pruebas realizadas por la OTI, debiendo generar la respectiva acta de evidencia.
- Verificar si se realizan respaldo de información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.

1.2. ACTIVIDADES DE EJECUCIÓN (DURANTE)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	OTI
Actividades de ejecución (durante)	R: Responsable I: Informado	E: Encargado	I: Informado	E: Encargado C: Consultado

- Evacuar el área, utilizando las rutas de emergencia de ser el caso.
- Únicamente si los expertos indican que es seguro, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado, de ser factible.
- Coordinar con la OTI para el corte del fluido eléctrico.
- Realizar el corte de fluido eléctrico a solicitud de la OTI.
- Paralizar los trabajos en altura a la intemperie.
- El personal deberá alejarse de las zonas inundadas por la lluvia.
- Si el evento sucede en horario fuera de las horas de trabajo, el personal de vigilancia de la OTI comunicará lo sucedido a la OTI.

1.3. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

ACTIVIDADES	RESPONSABLE			
	OTI	OTI	OTI	OTI
Actividades de recuperación (después)	I: Informado	E: Encargado	R: Responsable	C: Consultado

- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
- No ingresar al área afectada hasta que los expertos indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
- Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.
- Realizar las coordinaciones necesarias para evitar accidentes en las zonas afectadas.
- Brindar el apoyo necesario a la OTI para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.
- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución, debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de Contingencia (mejora continua) y actualizar las fichas de contingencia.