**RESOLUCIÓN DE CONSEJO UNIVERSITARIO N° 0350-2021**

Arequipa, 23 de julio de 2021.

Visto el Oficio Nº 0162-2021-OUIS-UNSA, de la Oficina Universitaria de Informática y Sistemas, mediante la cual solicitan se tenga a bien autorizar la aprobación del "Plan de Contingencias de Tecnologías de la Información."

**CONSIDERANDO:**

Que, la Universidad Nacional de San Agustín de Arequipa está constituida conforme a la Ley N° 30220, Ley Universitaria, y se rige por sus respectivos estatutos y reglamentos, siendo una comunidad académica orientada a la investigación y a la docencia, que brinda una formación humanista, ética, científica y tecnológica con una clara conciencia de nuestro país como realidad multicultural.



Que, el artículo 8° de la Ley N° 30220, Ley Universitaria, concordante con el artículo 8° del Estatuto Universitario, referente a la autonomía universitaria establece lo siguiente: *"(…) La Universidad se rige con la autonomía inherente a las Universidades y se ejerce de conformidad con lo establecido en la Constitución, la Ley y demás normativas aplicables. Esta autonomía se manifiesta en los siguientes regímenes: 8.1* ***Normativo****, implica la potestad autodeterminativa para la creación de norma internas (estatuto y reglamentos) destinados a regular la institución universitaria. 8.2* ***De gobierno****, implica la potestad autodeterminativa para estructurar, organizar y conducir la institución universitaria, con atención a su naturaleza, características y necesidades. Es formalmente dependiente del régimen normativo. 8.3* ***Académico****, implica la potestad autodeterminativa para fijar el marco del proceso de enseñanza-aprendizaje dentro de la institución universitaria. Supone el señalamiento de los planes de estudios, programas de investigación, formas de ingreso y de egreso de la institución y otros aspectos académicos. Es formalmente dependiente del régimen normativo y es la expresión más acabada de la razón de ser de la actividad universitaria. (…)".*

Que, el artículo 5° del Estatuto Universitario vigente, establece que: *"La Universidad tiene los siguientes fines: 5.1. Preservar, acrecentar y transmitir de modo permanente, la herencia científica, tecnológica, cultural y artística de la humanidad".*

Que, a través del documento del visto, la Oficina Universitaria de Informática y Sistemas, manifiesta que en atención a las recomendaciones dadas por la Sociedad Auditora (SOA) respecto a las Tecnologías de Información y Comunicaciones (TIC), solicita se tenga a bien autorizar la aprobación del Plan de Contingencias de Tecnologías de la Información.

Que, el mencionado Plan de Contingencias de Tecnologías de la Información, tiene como objetivo identificar las actividades que deberán ser realizadas ante determinadas contingencias a fin de poder dar continuidad a las operaciones de Tecnologías de la Información (TI) en la UNSA; estableciendo medidas técnicas y organizativas con el propósito de asegurar y restaurar los servicios que se brindan de forma rápida, eficiente y oportuna, minimizando el impacto (riesgo) negativo sobre los mismos.

Que, en consecuencia, el Consejo Universitario en su sesión del **26 de mayo de 2021**, acordó aprobar el Plan de Contingencias de Tecnologías de la Información de la Oficina

Universitaria de Informática y Sistemas de la Universidad Nacional de San Agustín de Arequipa, que formará parte integrante de la resolución a emitirse.

Por estas consideraciones y conforme a las atribuciones conferidas al Consejo Universitario por la Ley Universitaria Ley Nº 30220,

**SE RESUELVE:**

1. **APROBAR** el **Plan de Contingencias de Tecnologías de la Información** de la Oficina Universitaria de Informática y Sistemas de la Universidad Nacional de San Agustín de Arequipa, que forma parte integrante de la presente Resolución.

2. **ENCARGAR** al **Jefe de la Oficina Universitaria de Informática y Sistemas,** Funcionario Responsable de la Elaboración y Actualización del Portal de Transparencia en coordinación con el **Jefe de la Oficina Universitaria de Imagen Institucional,** la publicación de la presente Resolución en la Página Web de la Universidad.

**REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE (Fda.) Rohel Sánchez Sánchez Rector, (Fda.) Orlando Fredi Angulo Salas, Secretario General**

La que transcribo para conocimiento y demás fines

**ABOG. MARÍA DEL ROSARIO VEGA MONTOYA**
**SECRETARIA ADMINISTRATIVA**
**SECRETARÍA GENERAL DE LA UNSA**

*C.c.: RECTORADO, DIGA, SDL, SDF, ODO, OUIS, OUII y Archivo (exp).*
*Exp.: 1019056-2021 y 1015263*
*/hmoc*

CONTENIDO



Universidad Nacional de San Agustín de Arequipa – RECTORADO

Universidad Nacional de San Agustín de Arequipa – SECRETARÍA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

CONTENIDO

## I. PRESENTACIÓN

Siendo uno de los activos más importante de la Universidad Nacional de San Agustín de Arequipa (UNSA) la información que esta genera y almacena en sus diferentes ámbitos, la Oficina Universitaria de Informática y Sistemas (OUIS) y en el marco de las funciones definidas en el Reglamento de Organización y Funciones – ROF 2017 y en atención a la Resolución Ministerial Nro.028-2015-PCM donde son aprobados los "Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno" es elaborado el presente Plan de Contingencia de los servicios informáticos del centro de datos UNSA y dependencias universitarias del campus de la UNSA (en adelante Plan de Contingencia); para lo cual se ha tomado como referencia la "Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información" del Instituto Nacional de Estadística e Informática – INEI.

En este orden de ideas, el presente "Plan de Contingencia" es un instrumento de gestión que identifica las actividades a ser realizadas que permiten la continuidad de las operaciones de Tecnologías de la Información (TI) en la UNSA; estableciendo medidas técnicas y organizativas con el propósito de asegurar y restaurar los servicios informáticos de forma rápida, eficiente y oportuna, minimizando el impacto (riesgo) negativo sobre el mismo.

## II. GENERALIDADES

### II.1. OBJETIVO GENERAL

Identificar las actividades que deberán ser realizadas ante determinadas contingencias a fin de poder dar la continuidad de las operaciones de TI en la organización; estableciendo medidas técnicas y organizativas con el propósito de asegurar y restaurar los servicios que se brindan de forma rápida, eficiente y oportuna, minimizando el impacto (riesgo) negativo sobre los mismos.

### II.2. OBJETIVOS ESPECÍFICOS

a. Indicar los lineamientos a seguir para la recuperación de los servicios informáticos ante un desastre, incidencia o evento.
b. Continuar con la operatividad de las diferentes áreas de la UNSA que se hayan visto afectadas por una situación adversa relacionada a los servicios de TI.
c. Prevenir y minimizar la pérdida o la corrupción de información digital; así como el daño permanente a los recursos informáticos que dan continuidad a las operaciones de la UNSA.

### II.3. ALCANCE

El presente Plan de Contingencia tiene por alcance el identificar las estrategias a seguir para la recuperación de los servicios informáticos ante un desastre, incidencia o evento en la infraestructura tecnológica que se encuentra en el centro de datos de la UNSA y dependencias universitarias del campus.

### II.4. BASE LEGAL

- Ley Nº 27658 – Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 23716 – Ley de Control Interno de las Entidades del Estado.
- Resolución de Contraloría General Nº 320-2006-CG, aprueba las Normas de Control Interno del Sector Público.
- Guía práctica para el desarrollo de planes de contingencia de sistemas de información – INEI.
- Resolución Ministerial Nº 028-2015-PCM, Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- Resolución Ministerial Nº 004-2016-PCM, aprueban el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27000:2014 Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Oficio Nº 185-2020-DIGA, solicita elaboración de plan de contingencia y plan de continuidad del negocio de la universidad.

## III. SITUACIÓN ACTUAL DE LA OUIS

### III.1. MISIÓN

Damos el soporte informático necesario a la UNSA para el logro de sus objetivos en materia de infraestructura de redes y servidores, adquisición de activos informáticos, sistemas de información desarrollados por esta oficina y operatividad de equipos de usuario final.

### III.2. VISIÓN

Convertirnos en un referente a nivel de universidades por:

- Contar con infraestructura informática de punta y de plena utilización por parte de los usuarios en general.
- Uso de TIC que optimicen los tiempos de atención, reduzcan la huella de carbono y ponga a disposición de la comunidad agustina información que permita la investigación y toma de decisiones.
- Contar con personal altamente capacitado en las herramientas TIC que maneja la OUIS e identificado con brindar el mejor servicio al usuario final.

Todo esto en línea con hacer de la UNSA una universidad referente a nivel latinoamericano

Universidad Nacional de San Agustín de Arequipa RECTORADO

Universidad Nacional de San Agustín de Arequipa SECRETARIA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

III.3. ORGANIZACIÓN

La organización de la Oficina Universitaria de Informática y Sistemas, dependen directamente del Rectorado y cuenta con siete unidades orgánicas que son las suboficinas de: Apoyo Administrativo, Desarrollo de Sistemas, Soporte Técnico, Redes y Telecomunicaciones, Mesa de Ayuda, Registro, Publicaciones.

## IV. INFRAESTRUCTURA TECNOLÓGICA

### IV.1. CENTRO DE DATOS DE LA UNSA

El Centro de Datos se encuentra ubicado en una habitación del pabellón de la Escuela Profesional de Química, en el área de Ciencias Físicas, cuya infraestructura no es adecuada y no reúne las condiciones de seguridad ante la ocurrencia de un desastre, incidencia o evento.

En ese sentido, a fin de garantizar la disponibilidad de la información que alberga el centro de datos se hace necesario la construcción de la infraestructura física con un diseño de acuerdo a lo señalado en las normas internacionales de diseño y construcción de centros de datos tales como TIA-942. Este estándar está aprobado por TIA (Telecommunications Industry Association) y ANSI (American National Standards Institute).

### IV.2. SERVICIO DE COMUNICACIONES DE ÁREA EXTENSA (WAN)

La UNSA cuenta con sedes provinciales, las cuales no cuentan con una conexión a la sede principal, algunas de ellas realizan el acceso a los servidores de la Intranet utilizando VPN a través de una conexión a Internet.

### IV.3. SERVICIO DE COMUNICACIONES DE ÁREA METROPOLITANA (MAN)

La UNSA cuenta con sedes en la ciudad, de las cuales solo cuentan con interconexión con la sede principal:

- Sede Ciencias Sociales a través de fibra óptica.
- Sede Ciencias Biomédicas a través de radio enlace y VPN.
- Sede de Administración Central a través de radio enlace y VPN.
- Sede del Parque Industrial a través de radio enlace.

Las demás sedes no cuentan con una conexión a la sede principal, algunas de ellas realizan el acceso a los servidores de la Intranet utilizando un cliente de VPN a través de una conexión a Internet y algunas otras sedes no cuentan con ningún tipo de conexión.

### IV.4. SERVICIO DE COMUNICACIONES DE VOZ

La UNSA no cuenta con una central telefónica que pueda unificar la comunicación por voz. Algunas dependencias de las sedes cuentan con centrales telefónicas analógicas, otras con centrales IP, la mayoría de las

dependencias cuentan con líneas de telefonía básica PSTN (Red Telefónica Conmutada Pública) independientes.

IV.5. SERVICIO DE COMUNICACIONES DE ÁREA LOCAL (LAN)

Actualmente se cuenta con un cableado estructurado UTP de categoría 5, 5e, 6 y 6a, enlaces de fibra óptica, Access point (WiFi) y clientes VPN con sedes remotas en su sede principal. Sin embargo, la mayoría del mencionado cableado estructurado es de más de 15 años atrás y se requiere realizar una actualización y estandarización del cableado estructurado. Asimismo, los equipos de infraestructura de red requieren una renovación para soportar las actuales velocidades y tecnologías de la red LAN. También el sistema eléctrico que alimenta los gabinetes donde se encuentran los equipos de comunicación que forman parte de la infraestructura de red no cuenta con protección de pozo a tierra, UPS, transformador de aislamiento ni generador eléctrico. El grupo electrógeno de la sede principal sólo energiza a algunos pabellones del de la sede principal de Ciencias de Físicas incluido el centro de datos.

IV.6. SERVICIO DE INTERNET

Las dependencias universitarias de las sedes de la UNSA, tienen acceso a Internet a través de distintos contratos, cuyas velocidades y tipos de servicio son variables. Una vez se tenga una adecuada infraestructura de red LAN se podrán integrar a todas las dependencias y contar con un solo acceso a Internet con su contingencia adecuada. La sede principal de la UNSA cuenta con un servicio de Internet con un ancho de banda de 1.5Gbps desde el 12 de enero del 2020, el cual brinda el acceso a Internet básicamente a las sedes de Biomédicas, Ingenierías, Sociales y la Administración Central, cuyas dependencias universitarias se están migrando a este nuevo servicio de manera paulatina y de acuerdo a que las necesidades mínimas de infraestructura de red adecuadas se van implementando.

IV.7. SISTEMAS DE RESPALDO

La UNSA, al igual que los accesos a Internet, sus dependencias cuentan con sus propias aplicaciones y bases de datos, los cuales no se encuentran centralizados, se espera construir el nuevo data center para poder realizar esta integración de información y poder aplicar políticas de seguridad y respaldo integrales. La OUIS cuenta con un sistema de respaldo (backup) mixto (automatizado y manual) de información y máquinas virtuales, que garantizan la integridad de los activos de información digital a cargo de la OUIS. Dichos backups son realizados según lo detallado en el siguiente cuadro:

| Nro. | Descripción | Tipo |
|---|---|---|

Universidad Nacional de San Agustín de Arequipa – RECTORADO

Universidad Nacional de San Agustín de Arequipa – SECRETARÍA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

| | | |
|---|---|---|
| 1 | Archivos de configuración de aplicativos | Backup incremental |
| 2 | Código fuente de aplicativos | Backup incremental |
| 3 | Documentos adjuntos de aplicativos | Backup incremental |
| 4 | Archivos de unidades compartidas | Backup incremental |
| 5 | Configuraciones de equipos de red | Backup incremental |
| 6 | Motor de Base de datos | Full Backup |
| 7 | Máquinas virtuales principales | Full Backup |
| 8 | Equipos de infraestructura de red | Equipos en Spare |

Cuadro 01: Tipo de backup realizado.

IV.8. MOTOR DE BASE DE DATOS

La UNSA no cuenta con un motor de base institucional integrado, cada dependencia cuenta con sus propias bases de datos. La OUIS trabaja con bases de datos de software libre, MaríaDB, Postgresql, tanto para los ambientes de producción, pruebas y desarrollo.

IV.9. SISTEMA DE VIRTUALIZACIÓN: SERVIDORES Y ALMACENAMIENTO (CLUSTER)

El data center de la UNSA a cargo de la OUIS, cuenta con siete (07) servidores de altas prestaciones y dos (02) sistemas de almacenamiento; los cuales en conjunto forman dos cluster de virtualización de máquinas virtuales, en los cuales se encuentran los ambientes de desarrollo, pruebas y producción, incluido los servidores virtuales asignados a otras dependencias universitarias.

IV.10. SISTEMA DE ALIMENTACIÓN DE ENERGÍA ELÉCTRICA

El data center de la UNSA cuenta con una (01) UPS para la autonomía de treinta minutos (30min) a los equipos que se encuentran en el centro de datos, sin embargo, debido a su antigüedad de siete (07) años y al crecimiento de equipos conectados en el data center, requiere ser renovado, lo cual está considerado en la construcción del nuevo data center. También se cuenta con un generador eléctrico cuya capacidad y antigüedad no abastece los requerimientos actuales. La sede principal de Ingenierías, donde se ubica el data center, cuenta con un generador eléctrico el cual permite abastecer de fluido eléctrico cuando ocurre cortes de energía eléctrica por parte de la empresa prestadora del servicio o por eventuales contingencias. En las demás sedes y dependencias no cubiertas por el generador eléctrico no se cuenta con UPS ni Generador eléctrico en los gabinetes principales de comunicaciones.

IV.11. SEGURIDAD PERIMETRAL

La frontera fortificada de la infraestructura de red de la UNSA incluye un equipo de seguridad perimetral de marca Palo Alto modelo PA-3260 , provista por el operador del servicio de Internet, para la seguridad perimetral de la sede principal de la UNSA, el cual tiene las siguientes características:

- Filtrado web: Establece políticas de acceso web para los usuarios de la comunidad universitaria, evitando además su acceso a sitios conocidos de phishing y fuentes de malware.
- IPS: Realiza la detección de amenazas basada en firmas y anomalías del tráfico.
- VPN de acceso remoto: Permite la conexión remota de manera segura a las aplicaciones de la Intranet de la UNSA.
- Protección de ataques DoS: Para aislar e identificar actividad maliciosa en la red aplicando técnicas de protección y mitigación para evitar la denegación de los servicios.

IV.12. ADMINISTRADOR DEL USO DE ANCHO DE BANDA

Para realizar el control del uso de ancho de banda se cuenta con un equipo SINEFA modelo SF950, provista por el proveedor de servicios de Internet, con el fin de conocer en tiempo real cuánto ancho de banda está disponible, asignando dinámicamente ancho a las aplicaciones que más lo necesitan y evitando el tráfico innecesario a fin de prevenir colapsos en la red. Asimismo, se realiza el monitoreo del tráfico para controlar las conexiones entrantes y salientes, el protocolo que está manejando este tráfico de red, la dirección, qué estación de trabajo está provocando congestiones, los puertos utilizados y estadísticas de tráfico con un histórico detallado.

IV.13. SISTEMA DE CONTROL DE ANTIVIRUS

La implementación de un sistema de antivirus empresarial se tiene que implementar de manera urgente, puesto que todas las estaciones de trabajo no cuentan con una protección centralizada y adecuada, en la actualidad se utilizan programas gratuitos de control de virus informáticos.

## V. PLAN DE CONTINGENCIA DE LOS SERVICIOS INFORMÁTICOS DEL CENTRO DE DATOS DE LA UNSA.

V.1. METODOLOGÍA

El presente Plan de Contingencia ha sido elaborado tomando como base las fases definidas en la "Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información" publicada por el INEI. Es a partir de esta guía que son adoptadas las siguientes fases y son detalladas a continuación:

Universidad Nacional de San Agustín de Arequipa RECTORADO

Universidad Nacional de San Agustín de Arequipa SECRETARIA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

1) Identificación de Riesgos.
2) Estrategias para la recuperación de desastre, incidencia o evento.
3) Realización de pruebas (implementación).

Asimismo, las escalas a utilizar en el presente documento corresponden a:

ESCALA CUALITATIVA DE PROBABILIDAD

Constituye la representación de 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. |

Cuadro 02: Escala cualitativa de probabilidad

ESCALA CUANTITATIVA DE IMPACTO

El mismo diseño definido para la escala cualitativa es empleado para la escala cuantitativa, la cual 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. |

Cuadro 03: Escala cuantitativa de probabilidad

ESCALAS CUANTITATIVAS DE PROBABILIDAD E IMPACTO

A continuación, son descritas las escalas cuantitativas de probabilidad e impacto.

| PROBABILIDAD DE OCURRENCIA | NIVEL |
|---|---|
| 1 | Bajo |
| 2 | Medio |
| 3 | Alto |

| IMPACTO | NIVEL |
|---|---|
| 1 | Bajo |
| 2 | Medio |
| 3 | Alto |

Cuadro 04: Escalas cuantitativas de probabilidad e impacto

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 |

Cuadro 05: Evaluación y clasificación del riesgo

NIVELES DE RIESGO



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

| Nivel de Riesgo (cualitativo) | Nivel de Riesgo (cuantitativo) | Prioridad | Descripción |
|---|---|---|---|
| Riesgo Inaceptable | 9 | Muy Alta | Se requiere acción inmediata, planes de tratamiento requeridos, implementados y reportados a la alta dirección. |
| Riesgo Importante | 6 | Alta | Se requiere planes de tratamiento requeridos, 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. |

Cuadro 06: Niveles de riesgo

CUANTIFICACIÓN DE LOS RIESGOS

Los riesgos serán cuantificados de acuerdo a dos factores:

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

**RIESGO = PROBABILIDAD x IMPACTO**

## V.2. IDENTIFICACIÓN DE RIESGOS

ANÁLISIS DE RIESGOS

La UNSA está expuesta a riesgos que pueden ser causados por eventos fortuitos o por el mal uso de los recursos, pudiendo afectar los objetivos o las metas trazadas por la institución. En este sentido, la identificación de los riesgos se encuentran referidos a aquellos que afectan la seguridad del centro de datos y la infraestructura de red de datos de la Intranet, el cual trae como consecuencia la indisponibilidad, operación y continuidad de los servicios informáticos.

RELACIÓN DE LOS RIESGOS QUE PUEDEN AFECTAR AL CENTRO DE DATOS E INTRANET:

A continuación, son detallados riesgos identificados al centro de datos e Intranet de la UNSA, descritos a continuación:

| # | Riesgo identificado | Descripción del riesgo | Consecuencia |
|---|---|---|---|
| 1 | 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. |
| 2 | Inundación / aniego | Ocupación de agua en zonas que habitualmente están libres debido al desbordamiento de ríos, torrentes, lluvias torrenciales, deshielo, riegos entre otros. Cabe precisar que el Centro de Datos actual se encuentra ubicado en un primer piso por debajo del nivel de un canal de regadío. Además las ducterias subterráneas de comunicación entre los pabellones de las dependencias universitarias de las sedes, son susceptibles a inundaciones. | Equipos inservibles por el ingreso de agua al ambiente destinado para el centro de datos, canalizaciones subterráneas de comunicaciones de datos y gabinetes de comunicación de la Intranet en las diferentes sedes de la UNSA; generando la interrupción de todos los servicios que brinda. |
| 3 | Tormenta eléctrica | Situación de atención que se declara bajo determinadas condiciones climáticas que podrían generar descargas eléctricas atmosféricas. La caída de un rayo dentro de un radio de 8 a 16 kilómetros generan un valor mayor a 2000V/m. | Equipos inservibles por el ingreso de energía eléctrica retroalimentada por los cables de data, debido a que no se tiene una protección adecuada de pozos a tierra. Generando la interrupción de todos los servicios que brindan los equipos activos de la infraestructura de red. |
| 4 | Incendio | Ocurrencia de fuego no controlado que puede afectar los bienes. | Destrucción de los ambientes destinados para el centro de datos y/o gabinetes de comunicación de la Intranet, generando la interrupción de todos los servicios que brindan. |
| 5 | Vandalismo | Se refiere a atentados que podrían afectar o destruir las instalaciones, equipos, programas informáticos, datos, documentación, etc., por su función está expuesto a ser afectado. | Interrupción parcial o total de los servicios que brindan el centro de datos y los equipos de la infraestructura de red. |

Universidad Nacional de San Agustín de Arequipa RECTORADO

Universidad Nacional de San Agustín de Arequipa SECRETARIA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

| | | | |
|---|---|---|---|
| 6 | 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 UNSA en contra de la institución. |
| 7 | Intrusión de la red de datos | Ataques que provienen localmente o de Internet, originados por hackers, 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. |
| 8 | Falta de fluido eléctrico | Pérdida del suministro eléctrico en el centro de datos o gabinetes de comunicación de la Intranet. | Pérdida del suministro de energía eléctrica en el centro de datos y/o gabinetes de comunicaciones de la Intranet, pudiendo originar daño en los equipos sensibles, pérdida de información originando una interrupción en los servicios que brindan. |

Cuadro 07: Riesgos comunes que pueden afectar al centro de datos y/o Intranet.

CUANTIFICACIÓN DE LOS RIESGOS IDENTIFICADOS.

En el siguiente cuadro se detallan la clasificación de los riesgos identificados en atención a lo señalado en la metodología definida.

| MATRIZ DE PROBABILIDAD POR IMPACTO | | | | | |
|---|---|---|---|---|---|
| # | Riesgo identificado | Probabilidad (P) | Impacto (I) | (P)x(I) | Nivel de riesgo |
| 1 | Terremoto | 2 | 3 | 6 | Riesgo Importante |
| 2 | Inundación / aniego | 1 | 4 | 4 | Riesgo Moderado |
| 3 | Tormenta eléctrica | 1 | 4 | 4 | Riesgo Moderado |
| 4 | Incendio | 1 | 3 | 3 | Riesgo Moderado |
| 5 | Vandalismo | 1 | 2 | 2 | Riesgo Bajo |
| 6 | Fraude | 1 | 2 | 2 | Riesgo Bajo |
| 7 | Intrusión de la red de datos | 2 | 2 | 4 | Riesgo Moderado |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Falta de fluido eléctrico | 2 | 3 | 6 | Riesgo Importante |

Cuadro 08: 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.

## V.3. ESTRATEGIAS PARA LA RECUPERACIÓN DE DESASTRES

La generalización del uso de los medios electrónicos, informáticos y telemáticos supone beneficios, pero también riesgos asociados ante la ocurrencias 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 antes (preventivas), durante y después (reactivas).

### V.3.1. ACTIVIDADES PREVIAS AL DESASTRE (PREVENTIVAS)

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 UNSA. En ese sentido, se hace necesario el contar con la siguiente información:

a. SISTEMAS DE INFORMACIÓN.

La OUIS a través de la Sub Oficina de Desarrollo de Sistemas (SODS) deberá contar con una relación de los Sistemas de Información; dicha relación debe considerar la siguiente información:

- Nombre de la aplicación o Sistema, determinado por la SODS.
- Lenguaje con el que fue creado el Sistema, incluyendo la relación de librerías que lo conforman.
- Área usuaria, esto es la(s) dependencia(s) dueña del proceso sistematizado.
- Las unidades orgánicas y entidades, (internos/externos) que usan la información del Sistema.
- El volumen de los archivos (en MB) que trabaja el Sistema, si fuera el caso.
- El tamaño de las bases de datos (en MB).

Universidad Nacional de San Agustín de Arequipa RECTORADO

Universidad Nacional de San Agustín de Arequipa SECRETARIA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

- El volumen de transacciones mensuales que maneja el sistema.
- La(s) fecha(s) críticas, en las que la información es necesaria y debe estar disponible (por ejemplo, la fecha en la que determinada información se está procesando).

Con esta información deberá realizarse una lista priorizada (Ranking) de los Sistemas de Información necesarios para que la UNSA recupere la operatividad ininterrumpida en el desastre, incidente o evento (CONTINGENCIA).

b. HARDWARE DEL CENTRO DE DATOS.
   - La Sub Oficina de Soporte Técnico (SOST) y la Sub Oficina de Redes y Telecomunicaciones (SORT), 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).

c. 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:

| # | DESCRIPCIÓN |
|---|---|
| 1 | Archivos de configuración de aplicativos. |
| 2 | Código fuente de aplicativos. |
| 3 | Documentos adjuntos de aplicativos. |
| 4 | Archivos de unidades compartidas. |
| 5 | Motor de base de datos. |
| 6 | Software base de PC (OS, Browser, Ofimática,etc.). |
| 7 | Software base de servidores (OS, PHP, Java, etc.). |

Cuadro 09: Respaldo de información.

d. HARDWARE DE LA INFRAESTRUCTURA DE RED.

- Las SOST y SORT, deberán identificar y etiquetar los equipos de infraestructura de red de la Intranet y cableado estructurado, de acuerdo a la importancia del servicio de conectividad que brinda, para ser priorizados en caso de una contingencia o evento; para de esa forma tener los equipos adecuados en spare y reemplazarlos.
- La SORT deberá mantener un backup de los archivos de configuración de los equipos de la infraestructura de red, para restablecer en los equipos spare.
- La SOST deberá contar con el material y herramientas necesarias para el restablecimiento de la conectividad.

V.3.2. ACTIVIDADES DURANTE EL DESASTRE

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).

Universidad Nacional de San Agustín de Arequipa RECTORADO

Universidad Nacional de San Agustín de Arequipa SECRETARIA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

FORMACIÓN DEL EQUIPO OPERATIVO.

Deberán existir dos 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.

V.3.3. ACTIVIDADES DESPUÉS DEL DESASTRE, INCIDENTE O EVENTO

EVALUACIÓN DE DAÑOS.

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).

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 UNSA. El personal de la OUIS 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.

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 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 primera, la restauración de los servicios priorizados de TI del centro de datos.
- La segunda, es volver a contar con todos los servicios y los recursos informáticos, debiendo ser esta última etapa lo suficientemente rápida y eficiente en la medida de lo posible.

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 realizadas, que tan bien se hicieron, que tiempo tomaron, qué circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

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

RETROALIMENTACIÓN

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 funcionaron adecuadamente descritas en las fichas de contingencia.

### V.4. REALIZACIÓN DE PRUEBAS (IMPLEMENTACIÓN)

FORMACIÓN DE EQUIPOS OPERATIVOS PARA LA REALIZACIÓN DE PRUEBAS

El equipo operativo será conformado por los colaboradores que serán designados por la OUIS y el oficial de seguridad de la información, 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).

## VI. DISPOSICIONES FINALES

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.
2. Realizar la conformación de un Comité el encargado de planificar, implementar y supervisar la ejecución del Plan de Contingencia, que asegure la legalidad, consistencia, adecuado uso, seguridad, inviolabilidad y sostenibilidad de los Sistemas de Información, hardware y software.
3. La actualización del presente plan de contingencia debe ser realizada una vez al año.
4. Todos los colaboradores que laboran en la UNSA, deben formar parte de las actividades y están obligados a participar en la implementación y ejecución del Plan de Contingencias de TI.

Universidad Nacional de San Agustín de Arequipa RECTORADO

Universidad Nacional de San Agustín de Arequipa SECRETARIA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

5. Definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento del Plan de Contingencia.
6. Las medidas que debemos adoptar para protegernos son tantas como amenazas existen, es por ello que se debe difundir a todas las unidades orgánicas el presente plan de contingencia.
7. Realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Plan de Contingencia, y así cumplir con las disposiciones legales vigentes dispuestas por la UNSA.
8. Contar con un centro de datos nuevo acorde a los estándares y con el avance de las tecnologías actuales. Además se debe prever contar con una subestación eléctrica y grupo electrógeno exclusivos para el centro de datos con transferencia de energía automática.
9. Contar con un centro de datos alterno a fin de minimizar el tiempo de recuperación de los servicios de TI.
10. Contar con equipos de infraestructura de red de repuesto (spare), materiales y herramientas para cableado estructurado, a fin de minimizar el tiempo de recuperación de los servicios de TI en la Intranet de la UNSA.

ANEXO 1.

RELACIÓN DE SISTEMAS DE INFORMACIÓN Y SU BASE DE DATOS EN PRODUCCIÓN

| ID | Nombre de la Aplicación | Plataforma – Arquitectura de Desarrollo | Base de Datos | Componentes de Seguridad |
|---|---|---|---|---|
| SI01 | Sistema de Admisión Pregrado | Php 4 ,javascript ,css, htm | MySQL | SODS |
| SI02 | Sistema de Admisión Postgrado | Php 4 ,javascript ,css, htm | MySQL | SODS |
| SI03 | Sistema de Calificación | Php 4 ,javascript ,css, htm | MySQL | SODS |
| SI04 | Sistema de caja | Php 4 ,javascript ,css, htm | MySQL | SODS |
| SI05 | Sistema de dependencias y centros de costos | Php 4 ,javascript ,css, htm | MySQL | SODS |
| SI06 | Sistema de comedor | Php 4 ,javascript ,css, htm | MySQL | SODS |
| SI07 | Sistema académico | Php 4 ,javascript ,css, htm | MySQL | DUFA |
| SI08 | Sistema tramited | php laravel view boostrap java script | postgress | SODS |
| SI09 | Aplicativo Libro de Reclamaciones | php laravel view boostrap java script | postgress | SODS |
| SI10 | Aplicativo Inscripcione OPACDR | php laravel view boostrap java script | postgress | SODS |
| S11 | Sistema Evote | NoteJS javascript | postgress | SODS |
| S12 | Sismo | Java | postgress | SODS |

ANEXO 2.

COORDINACIÓN EQUIPO DE RESPUESTA A EMERGENCIA EN EL CENTRO DE DATOS E INTRANET

| Nro. | Nombre de personal | Cargo | Celular |
|---|---|---|---|
| 1 | Lizardo Pérez Cerpa | Oficial de Seguridad de la Información | 939 086 692 |

| | | | |
|---|---|---|---|
| 2 | Álvaro Montes de Oca Beltrán | Jefe(a) de la OUIS | 939 085 544 |
| 3 | Alberto Valdivia Arévalo | Jefe(a) de la SOST | 959 614 466 |
| 4 | Boris Verástegui Bustamante | Jefe(a) de la SORT | 950 700 000 |

LISTADO DE PERSONAL: EQUIPO DE RESPUESTA DE EMERGENCIA DE SEGURIDAD PERIMETRAL

| Nro. | Nombre de personal | Cargo | Celular |
|---|---|---|---|
| 1 | Lizardo Pérez Cerpa | Oficial de Seguridad de la Información | 939 086 692 |
| 2 | Boris Verástegui Bustamante | Jefe(a) de la SORT | 950 700 000 |
| 3 | Diana Pizarro | ISP - ejecutivo postventa | 997 109 301 |

LISTADO DE PERSONAL: EQUIPO DE RESPUESTA A EMERGENCIA DEL CENTRO DE DATOS

| Nro. | Nombre de personal | Cargo | Celular |
|---|---|---|---|
| 1 | Lizardo Pérez Cerpa | Oficial de Seguridad de la Información | 939 086 692 |
| 2 | Álvaro Montes de Oca Beltrán | Jefe(a) de la OUIS | 939 085 544 |
| 3 | Alberto Valdivia Arévalo | Jefe(a) de la SOST | 959 614 466 |
| 4 | Boris Verástegui Bustamante | Jefe(a) de la SORT | 950 700 000 |

LISTADO DE PERSONAL: EQUIPO DE RESPUESTA A EMERGENCIA DE LA INTRANET

| Nro. | Nombre de personal | Cargo | Celular |
|---|---|---|---|
| 1 | Alberto Valdivia Arévalo | Jefe(a) de la SOST | 959 614 466 |
| 2 | Boris Verástegui Bustamante | Jefe(a) de la SORT | 950 700 000 |

LISTADO DE PROVEEDORES

| Nro. | Nombre de personal | Cargo | Celular |
|---|---|---|---|
| 1 | Diana Pizarro | ISP - ejecutivo postventa | 997 109 301 |
| 2 | | Cableado Estructurado | |
| 3 | | Radio enlaces | |
| 4 | | Equipos de Infraestructura de red | |

ANEXO 3.

| PROCESO: OUIS.2020.1 Gestión de Data Center | Código: FC-001 |
|---|---|
| **RIESGO: INTRUSIÓN** | |
| 1. DESCRIPCIÓN DEL EVENTO.<br>Ataques que provienen desde Internet, originados por hackers, virus con la finalidad de alterar el normal funcionamiento de los recursos informáticos, malware, etc. | |
| 2. ACTIVIDADES DE PREVENCIÓN (ANTES).<br>MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES | |
| | RESPONSABLE |

| ACTIVIDADES | OUIS | SODS/SORT | OFICIAL DE SEGURIDAD | RECTOR |
|---|---|---|---|---|
| Actividades preventivas (antes) | C | E | R | I |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE DESARROLLO DE SISTEMAS (SODS) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Contar con respaldos actualizados de los datos electrónicos de la UNSA, almacenados fuera del inmueble y/o en un servidor remoto.
b. Contar con los equipos de seguridad perimetral actualizados y con soporte vigente.
c. Contar con antivirus instalados en las PC's y Servidores, actualizados y con soporte vigente.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Verificar se realicen respaldos de la información de manera periódica por la SODS y SORT, debiendo generar la respectiva acta de evidencia.
b. Verificar que cuente con la actualización y el soporte vigente del Firewall-NG y antivirus, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SODS/SO | OFICIALD | RECTOR |

| | | RT | ESEGURIDAD | |
|---|---|---|---|---|
| Actividades de ejecución (durante) | IC | E | CR | I |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE DESARROLLO DE SISTEMAS (SODS) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Confirmada la presencia de una intrusión en la red, se deberá investigar su origen para lo cual se debe comprobar cuales son los equipos y servicios que están siendo comprometidos a fin de identificar los causantes del ataque.
b. Visualizar los procesos activos en los servidores a fin de identificar 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 UNSA.
c. 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.
d. Chequeo de los archivos binarios del sistema a fin de detectar si han sido modificados.
e. Comprobar los puertos de conexión abiertos; a fin de detectar si hay alguno en especial que no lo debería ser.
f. Analizar los directorios FTP/HTTP/HTTPS/SMB a fin de detectar si alguno de ellos ha podido ser escrito por usuarios anónimos.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Realizar el monitoreo del incidente.

4. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SODS/ | OFICI | RECT |

| | | | | |
|---|---|---|---|---|
| | | SORT | ALDESEGURIDAD | OR |
| Actividades de recuperación (después) | I | E | CR | IC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE DESARROLLO DE SISTEMAS (SODS) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. 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.
b. Realizar un análisis forense de la intrusión en la red a fin de diseñar nuevas medidas que eviten incidentes futuros parecidos.
c. 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.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Registrar lo sucedido; así como las actividades que fueron realizadas para su solución, debiendo llevar un control del mismo e informar al RECTOR.
b. Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.

OFICINA UNIVERSITARIA DE INFORMÁTICA Y SISTEMAS

a. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

| PROCESO: OUIS.2020.1 Gestión de Data Center | Código: FC-002 |
|---|---|
| **RIESGO: TERREMOTO** | |
| 1. DESCRIPCIÓN DEL EVENTO.<br>Fenómeno natural manifestado por una sacudida brusca de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas sísmicas. | |
| 2. ACTIVIDADES DE PREVENCIÓN (ANTES). | |

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades preventivas (antes) | I | E | R | EC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB DIRECCIÓN DE INFRAESTRUCTURA (SDI)

a. Revisar una vez al año la infraestructura donde se encuentra el centro de datos.

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS

SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Contar con respaldos actualizados de los datos electrónicos de la UNSA, almacenados fuera del inmueble y/o en un servidor remoto.
b. Asegurar que los elementos que se encuentran 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.
c. Se mantendrán cerradas las puertas de los gabinetes a fin de minimizar la caída de equipos u otros.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Verificar la ejecución de las pruebas realizadas por la Sub Dirección de Infraestructura, debiendo generar la respectiva acta de evidencia.
b. Verificar se realicen respaldos de la información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades de ejecución (durante) | RI | E | I | EC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS

SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Evacuar el área si es necesario, utilizando las rutas de emergencia buscando un lugar seguro y evitando ventanas, así como el uso de escaleras.
b. Coordinar con la Sub Dirección de Infraestructura el corte del fluido eléctrico.

SUBDIRECCIÓN DE INFRAESTRUCTURA

a. Si el evento sucede en horario fuera de horas de trabajo, el personal de la Oficina de Vigilancia de la UNSA comunicará lo sucedido al "equipo de respuesta de emergencia de Centro de Datos".

4. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/S | OFICIA | SDI |

| | | | | |
|---|---|---|---|---|
| | | ORT | LDESEGURIDAD | |
| Actividades de recuperación (después) | I | E | R | C |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE DESARROLLO DE SISTEMAS (SODS) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
b. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
c. 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.

SUBDIRECCIÓN DE INFRAESTRUCTURA.

a. Ante la posibilidad de un incendio, a solicitud de la OUIS realizar el corte de fluido eléctrico y/o cerrar el paso de agua aledañas al centro de datos.
b. Brindar el apoyo necesario a la OUIS para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. 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.
b. Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.

OFICINA UNIVERSITARIA DE INFORMÁTICA Y SISTEMAS

a. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

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.

2. ACTIVIDADES DE PREVENCIÓN (ANTES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades preventivas (antes) | I | I | R | EC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB DIRECCIÓN DE INFRAESTRUCTURA (SDI)

a. Revisar una vez al año el espacio físico donde se encuentra el centro de datos para descartar la existencia de filtraciones de agua.
b. Revisar una vez al año los sistemas de desagüe y drenaje en el área circundante al centro de datos.
c. Contratar una vez al año la revisión y mantenimiento de las alarmas de inundación o aniego.
d. Señalizar las llaves de paso de agua al centro de datos.

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS

SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Contar con respaldos actualizados de los datos electrónicos de la UNSA, almacenados fuera del inmueble y/o en un servidor remoto.
b. Verificar que los cables del cableado estructurado no se encuentren expuestos a posibles inundaciones o aniegos.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Verificar la ejecución de las pruebas realizadas por la Sub Dirección de Infraestructura, debiendo generar la respectiva acta de evidencia.
b. Verificar se realicen respaldos de la información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIAL DE SEGURIDAD | SDI |
| Actividades de ejecución (durante) | RI | E | I | EC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Evacuar el área, utilizando las rutas de emergencia de ser el caso.
b. Únicamente si las brigadas y/o autoridades indiquen que es seguro, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado, de ser factible.
c. Coordinar con la Sub Dirección de Infraestructura el corte del fluido eléctrico.

SUB DIRECCIÓN DE INFRAESTRUCTURA

a. Realizar el corte de fluido eléctrico a solicitud de la OUIS.
b. Si el agua proviene del interior cerrar las llaves de paso que sean necesarias.
c. Si el agua proviene del exterior, cerrar las llaves de paso que sean necesarias y bloquear las entradas de agua.

Universidad Nacional de San Agustín de Arequipa – RECTORADO

Universidad Nacional de San Agustín de Arequipa – SECRETARIA GENERAL



Santa Catalina 117, Arequipa, Perú — Teléfono (51 54) 224903. E-mail: secgen@unsa.edu.pe

d. Si el evento sucede en horario fuera de horas de trabajo, el personal de la Oficina de Vigilancia de la UNSA comunicará lo sucedido al "equipo de respuesta de emergencia de Centro de Datos".

4. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades de recuperación (después) | I | E | R | C |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE DESARROLLO DE SISTEMAS (SODS) – OUIS

SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
b. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
c. 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.

SUB DIRECCIÓN DE INFRAESTRUCTURA.

a. Realizar las coordinaciones necesarias para extraer el agua y/o humedad de las zonas afectadas.
b. Brindar el apoyo necesario a la OUIS para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. 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.
b. Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.

OFICINA UNIVERSITARIA DE INFORMÁTICA Y SISTEMAS

a. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

| PROCESO: OUIS.2020.1 Gestión de Data Center | Código: FC-004 |
|---|---|
| RIESGO: INCENDIO | |

1. DESCRIPCIÓN DEL EVENTO.

Ocurrencia de fuego no controlado que puede afectar los bienes.

2. ACTIVIDADES DE PREVENCIÓN (ANTES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades preventivas (antes) | I | E | R | EC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB DIRECCIÓN DE INFRAESTRUCTURA (SDI)

a. Programar una vez al año la revisión y mantenimiento de alarmas contra incendios.

b. Programar una vez al año la recarga de extintores y la capacitación del personal en el uso de los mismos.

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Contar con respaldos actualizados de los datos electrónicos de la UNSA, almacenados fuera del inmueble y/o en un servidor remoto.
b. Verificar que los cables del cableado estructurado no se encuentren cerca a posibles fuentes de calor.
c. Verificar una vez al año que el cableado eléctrico y tomas eléctricas se encuentren en condiciones óptimas de operación.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Verificar la ejecución de las pruebas realizadas por la Sub Dirección de Infraestructura, debiendo generar la respectiva acta de evidencia.
b. Verificar se realicen respaldos de la información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.
c. Verificar la ejecución de las pruebas realizadas por las SOST y SORT, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades de ejecución (durante) | R | E | I | C |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Evacuar el área, utilizando las rutas de emergencia de ser el caso.
b. Alertar a los Bomberos, para ello se recurrirá a los números telefónicos de emergencia, a efectos de obtener una pronta respuesta al acontecimiento.
c. Únicamente si existen las condiciones de seguridad, desconectar los equipos de comunicaciones, servidores y sistemas de almacenamiento del centro de datos considerando su correcto apagado de ser factible.
d. Coordinar con la Sub Dirección de Infraestructura el corte del fluido eléctrico.

SUB DIRECCIÓN DE INFRAESTRUCTURA

a. Realizar el corte de fluido eléctrico a solicitud de la OUIS.
b. Si el evento sucede en horario fuera de horas de trabajo, el personal de la Oficina de Vigilancia de la UNSA comunicará lo sucedido al "equipo de respuesta de emergencia de Centro de Datos".

4. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades de recuperación (después) | I | E | R | C |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE DESARROLLO DE SISTEMAS (SODS) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.

b. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
c. 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.

SUB DIRECCIÓN DE INFRAESTRUCTURA.

a. Brindar el apoyo necesario a la OUIS para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. 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.
b. Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.

OFICINA UNIVERSITARIA DE INFORMÁTICA Y SISTEMAS

a. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

| PROCESO: OUIS.2020.1 Gestión de Data Center | Código: FC-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 (03) niveles de Alerta:

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

2. ACTIVIDADES DE PREVENCIÓN (ANTES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades preventivas (antes) | I | I | R | EC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB DIRECCIÓN DE INFRAESTRUCTURA (SDI)

a. Asegurar que todas las instalaciones contra tormentas eléctricas estén identificados y adecuadamente señalizados.
b. Asegurar que todo el personal este adecuadamente entrenados.
c. Asegurar que los contratistas que trabajan cumplan o excedan con lo indicado en el presente estándar.
d. Verificar y dar mantenimiento a los refugios instalados en el campus universitario.

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Contar con respaldos actualizados de los datos electrónicos de la UNSA, almacenados fuera del inmueble y/o en un servidor remoto.
b. Verificar que los cables del cableado estructurado no se encuentren expuestos a posibles inundaciones o aniegos.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Realizará la coordinación con las áreas involucradas para realizar las pruebas e inspección de las alarmas sonoras y visuales.
b. Verificar la ejecución de las pruebas realizadas por la Sub Dirección de Infraestructura, debiendo generar la respectiva acta de evidencia.

c. Verificar se realicen respaldos de la información de manera periódica por las SODS y SORT, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIAL DE SEGURIDAD | SDI |
| Actividades de ejecución (durante) | RI | E | I | EC |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE SOPORTE TÉCNICO (SOST) – OUIS

SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Evacuar el área, utilizando las rutas de emergencia de ser el caso.
b. Únicamente si las brigadas y/o autoridades indiquen que es seguro, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado, de ser factible.
c. Coordinar con la Sub Dirección de Infraestructura el corte del fluido eléctrico.

SUB DIRECCIÓN DE INFRAESTRUCTURA

a. Realizar el corte de fluido eléctrico a solicitud de la OUIS.
b. Paralizar los trabajos en altura a la intemperie.
c. El personal deberá alejarse de charcos o zonas inundadas por la lluvia.
d. Si el evento sucede en horario fuera de horas de trabajo, el personal de la Oficina de Vigilancia de la UNSA comunicará lo sucedido al "equipo de respuesta de emergencia de Centro de Datos".

4. ACTIVIDADES DE RECUPERACIÓN (DESPUÉS)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

| | RESPONSABLE | | | |
|---|---|---|---|---|
| ACTIVIDADES | OUIS | SOST/SORT | OFICIALDESEGURIDAD | SDI |
| Actividades de recuperación (después) | I | E | R | C |

E: Encargado, R: Responsable, C: Consultado, I: Informado

SUB OFICINA DE DESARROLLO DE SISTEMAS (SODS) – OUIS
SUB OFICINA DE REDES Y TELECOMUNICACIONES (SORT) – OUIS

a. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
b. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si se cuenta con la protección necesaria.
c. 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.

SUB DIRECCIÓN DE INFRAESTRUCTURA.

a. Realizar las coordinaciones necesarias para evitar accidentes en las zonas afectadas.
b. Brindar el apoyo necesario a la OUIS para el traslado de los equipos de comunicación, servidores y sistemas de almacenamiento a un lugar seguro.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. 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.
b. Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.

OFICINA UNIVERSITARIA DE INFORMÁTICA Y SISTEMAS

a. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.