*Segunda Conferencia de Directores de Tecnologías de Información y Comunicación de Instituciones de Educación Superior, Lima, 2 y 3 de Julio de 2012*

# Caso de Éxito: Implementación del Marco de Trabajo de Continuidad de la Infraestructura de TI de ARANDU - PARAGUAY

Carlos Luis Filippi, Emilse Serafini de Carou

Universidad Nacional de Asunción, Centro Nacional de Computación, Senador Dr. José Decoud casi Dr. Carlos Zubizarreta ï Campus de la UNA ï San Lorenzo
director@cnc.una.py, eserafini@cnc.una.py

**Resumen.** Es indudable la importancia de los servicios que las Redes Académicas o Redes Nacionales de Investigación y Educación, ponen a disposición de investigadores y académicos de todo el mundo, permitiéndoles una nueva manera de colaborar y compartir información y recursos, eliminando, además, las barreras temporales y espaciales. ARANDU, la Red Académica Paraguaya, apunta hacia la implementación de servicios con interrupciones mínimas, para lo cual elaboró un Plan de Continuidad del Negocio, preparándose de forma responsable y seria ante los desafíos que propone una contingencia y los requerimientos de los usuarios.

**Palabras Clave:** ARANDU, Plan de Continuidad del Negocio, contingencia.

## 1 Introducción

La implementación de ARANDU[1] nace de una iniciativa impulsada por la Universidad Nacional de Asunción, para la interconexión de las universidades y los centros de investigación del Paraguay.

En el 2002, miembros del Centro Nacional de Computación de la Universidad Nacional de Asunción, participaron en las reuniones y grupos de trabajo de las NRENs (National Research and Education Network) latinoamericanos y firman la declaración de Toledo sobre Redes de Investigación y Educación en América Latina. Más tarde, en el 2003, suscriben el Acta Constitutiva de CLARA (Cooperación Latinoamericana de Redes Avanzadas).

El 17 de octubre de 2011, bajo la denominación ñRED ACADEMICA PARA LA CIENCIA, LA EDUCACION Y LA TECNOLOGIA ARANDUò, por mandato y voluntad de la Universidad Nacional de Asunción, la Universidad Católica ñNuestra Señora de la Asunciónò, la Universidad Nacional del Este, la Universidad Autónoma de Asunción, la Compañía Paraguaya de Comunicaciones S.A. (COPACO S.A.) y la Fundación Parque Tecnológico Itaipu Paraguay, fue constituida una asociación reconocida de utilidad pública y sin fines de lucro, firmándose el Acta Fundacional y constituyéndose la primera Comisión Directiva.

[1] Palabra guaraní que significa Sabiduría, Sabio.

Actualmente, ARANDU interconecta a sus miembros y, próximamente, concretará su conexión a la RedCLARA.

La infraestructura tecnológica necesaria para el funcionamiento del Centro de Operaciones de Red de ARANDU y la contratación de una Consultoría para la elaboración del Plan de Continuidad del Negocio, fue obtenida gracias al Proyecto Mercosur Digital[2], en su Vertiente Red de Capacitación Digital, eje Plataforma Tecnológica y Apoyo a Paraguay.

ARANDU es consciente que durante las actividades cotidianas que desarrollará, pueden presentarse situaciones que afectarían la normal provisión de servicios. Por tanto, se prepara de forma responsable y seria para afrontar y superar las diferentes emergencias y consecuencias de las mismas, apuntando a la planeación de la continuidad de la provisión de servicios.

Para garantizar que la infraestructura de Tecnología de Información (TI) de ARANDU pueda continuar suministrando servicios (especialmente aquellos considerados críticos) o puedan ser recuperados en un tiempo adecuado en caso de que se produzca una interrupción, fue elaborado, en el contexto de la Consultoría mencionada más arriba, un Marco de Trabajo de Continuidad de la Infraestructura de TI, conteniendo las Políticas de Seguridad y el Plan de Contingencias.

Este documento tiene como objetivo presentar el Caso de Éxito de la implementación del Marco de Trabajo de Continuidad de la Infraestructura de TI de ARANDU.

## 2 Marco General del Plan de Continuidad del Negocio (BCP, Business Continuity Plan)

El BCP es un plan de procedimientos alternativos a la forma tradicional de operar de cualquier organización o empresa y es una herramienta que ayuda a que los procesos que se consideran críticos continúen funcionando durante una interrupción. Un Plan de Continuidad del Negocio, se enfoca en sostener las funciones del negocio durante y después de una interrupción a los procesos críticos de la organización, identifica las amenazas potenciales y los impactos a las operaciones que esas amenazas, podrían causar si se llegaran a materializar.

En el marco del Plan de Continuidad del Negocio, ARANDU deberá:

- Administrar eficientemente el Plan
- Infundir confianza en el equipo de trabajo y los miembros de la Red hacia su habilidad para manejar las interrupciones que pudieran darse
- Incrementar su capacidad de respuesta en el menor tiempo posible
- Minimizar el impacto y la probabilidad de las interrupciones

Estos beneficios se materializarán mediante un entrenamiento y sensibilización constantes en todos los niveles de ARANDU, incluyendo a sus miembros, para lograr efectos duraderos.

Un Plan de Continuidad del Negocio exitoso depende de la correcta identificación de roles y asignación de responsabilidades claramente definidas para su gestión, para

[2] Proyecto Mercosur Digital, www.mercosurdigital.org

asegurar que las tareas requeridas para implementar y mantener el Plan están asignadas a personas competentes y se realizarán en forma correcta.

Estos puntos fueron abordados para la elaboración del Plan de Continuidad del Negocio de ARANDU.

## 3 Marco de Trabajo de Continuidad de la Infraestructura de TI

El desarrollo del Marco de Trabajo tiene como propósito principal establecer la capacidad estratégica y táctica de ARANDU para la planificación y respuesta a incidentes e interrupciones de la operatoria diaria de la Red, con el objeto de mantener el funcionamiento de los servicios brindados a un nivel aceptable, previamente definido, identificando amenazas potenciales y posibles impactos en las operaciones.

Durante el desarrollo del Marco de Trabajo fueron delineadas las siguientes Fases:

- FASE I: Obtención del Conocimiento
- FASE II: Formalización de Procesos de Seguridad de la Infraestructura de TI de ARANDU
- FASE III: Garantía de Continuidad del Servicio
- FASE IV: Entrenamiento
- FASE V: Evaluación de la Implementación

### 3.1 Fase I: Obtención del Conocimiento

Durante esta etapa se realizó un Relevamiento Inicial de las instalaciones y servicios de ARANDU.

Las herramientas utilizadas para la obtención del conocimiento fueron:

- Análisis de Impacto en el negocio: evaluación del impacto en el tiempo, de una interrupción sobre la capacidad de ARANDU para operar.
- Análisis de Requerimientos de Continuidad: estimación de los recursos, instalaciones y servicios externos que cada actividad requerirá en la reanudación y retorno a la operatoria normal luego de una interrupción.
- Evaluación de Amenazas por medio del Análisis de Riesgo: estimación de la probabilidad y el impacto de amenazas conocidas sobre funciones específicas.

El Relevamiento permitió obtener un conocimiento global de todos los servicios operativos involucrados, niveles de criticidad y personas involucradas en los mismos.

### 3.2 Objetivo General

El objetivo general de la FASE I fue evaluar la Seguridad General y Física de las instalaciones donde está alojado el equipamiento tecnológico de ARANDU para, posteriormente, definir los delineamientos que direccionen y apoyen la seguridad de la infraestructura tecnológica de la Red, con el fin de garantizar que se cumplan los requisitos especificados para la disponibilidad de servicios.

### 3.3 Alcance de la Fase I

La evaluación fue centrada en la verificación del cumplimiento de los Indicadores componentes de la Estructura de Gestión y Control Interno, clasificada por los Ámbitos de Administración relacionadas a cada aspecto evaluado:

I. ADMINISTRACIÓN DE LAS INSTALACIONES
   A. Infraestructura Edilicia
   B. Continuidad del Servicio
II. ADMINISTRACIÓN DE LA SEGURIDAD / PREVENCIÓN DE INCENDIOS
   C. Servicios de Seguridad
   D. Dispositivos/Elementos de Seguridad
   E. Prevención contra incendios
III. ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA
   F. Sala Técnica y/o Data Center

Los trabajos de verificación de los Indicadores de Gestión fueron desarrollados en la infraestructura edilicia y tecnológica del Centro Nacional de Computación, incluyendo las siguientes áreas:

- Área Técnica:
  - CPD ï Centro de Procesamiento de Datos
  - Jefatura del Área Técnica
  - Área de Desarrollo
  - Área de Comunicaciones
  - Taller de Soporte Técnico y Mantenimiento
  - Área Soporte Internet, Punto.Py
- Edificio del Centro Nacional de Computación en general

### 3.4 Normas Aplicadas

Fueron aplicadas las siguientes Normativas, Circulares Internas y Reglamentaciones vigentes en la República del Paraguay:

- Manual de Control Interno Informático para Entidades Financieras (MCIIEF)[3], considerando los Objetivos de Control de Alto Nivel y Detallados relacionados a la Seguridad General, Física y a la Administración de las Instalaciones.
- Ordenanzas Municipales:
  - Nro. 26.104/91 ñAprobación de Planos y Habilitación Municipalò
  - Nro. 25.097/98 ñNormas generales y particulares de Seguridad y Prevención contra Incendiosò
  - Nro. 44/98 ñFiscalización de las Instalaciones Eléctricas y Electromecánicas en Edificios en general e industriasò.
- Acuerdos y Contratos con Proveedores de Servicios: Instalaciones Eléctricas, Aires Acondicionados, Instalaciones Lógicas, Limpieza, Guardias de Seguridad y Monitoreo.

[3] Emitido por la Superintendencia de Bancos del Banco Central del Paraguay por Resolución SB. SG. Nro. 00188/2002

- Modelo de Objetivos de Control para la Información y Tecnologías relacionadas (CobiT®[4]) - Marco de Referencia Internacional- Control Interno, Seguridad Física y de las Instalaciones y Control de Acceso.
- ISO 27001 - Certificación de Calidad para la Seguridad en Tecnología de Información.

### 3.5 Metodología de Trabajo

Para la ejecución de la Fase I fueron utilizadas las Planillas de Evaluación de la Seguridad General y Física y las Documentaciones suministradas por la Dirección General, el Área Técnica y el Encargado del Taller de Soporte Técnico y Mantenimiento de la Infraestructura Tecnológica del CNC.

Las Planillas de Evaluación fueron diseñadas para que las áreas de Soporte y Mantenimiento Técnico adopten las mismas como una Herramienta de Gestión para la supervisión periódica del Servicio de Proveedores y puntos de verificación para la habilitación de nuevas Áreas.

| I ADMINISTRACIÓN DE INSTALACIONES | Estado | N 1 Punto | N2 Parcial Punto | N3 Prom. Comp. | N4 Prom. Parcial | Prom. Gral. |
|---|---|---|---|---|---|---|
| A.- Infraestructura Edilicia: | | | | | | 2,30 |
| 1 Ubicación Física | | | | | 3,00 | |
| a) Estación de Servicio | | | | 3,00 | | |
| 2 Planos y Habilitación Municipal | | | | | 1,00 | |
| a) Arquitectónico | | | | 1,00 | | |
| b) Prevención de Incendios | | | | 1,00 | | |
| c) Plano de Instalaciones Eléctricas | | | | 1,00 | | |
| 3 Instalaciones Eléctricas | | | | | 2,31 | |
| a) Mantenimiento Mensual - Contrato | | | | 2,31 | | |
| i.- Ficha de Servicio | | | 2,67 | | | |
| 1.- Existencia | | 3 | | | | |
| 2.- Descripción del Servicio | | 3 | | | | |
| 3.- Firma del Responsable de la Agencia | | 2 | | | | |
| ii.- Tablero Principal | | | 2,40 | | | |
| 1.- Cartel Indicador | | 1 | | | | |
| 2.- Porta Plano | | 2 | | | | |
| 3.- Contrafrente | | 3 | | | | |
| 4.- Espacio No Utilizado | | 3 | | | | |

**Fig. 1.** Evaluación de la Seguridad General y Física de la Infraestructura de ARANDU

### 3.6 Tareas Realizadas

La implementación de ARANDU se encuentra apoyada por la gestión del Control Interno, el cual encaminó al diseño e implementación de Políticas y Directrices que

[4] Objetivos de control para la información y tecnologías relacionadas, es una metodología publicada en 1996 por el Instituto de Control de TI e ISACA (Asociación de Auditoría y Control de Sistemas de Información).

aseguran el cumplimiento de los objetivos de la organización y la mitigación de los riesgos a los que pudiera estar expuesta.

En este contexto, fueron desarrolladas las siguientes tareas:

- Determinación de Indicadores de Gestión y Control Interno en consideración a las Normativas vigentes relacionadas a la Administración de las Instalaciones, Seguridad y Prevención contra Incendios e Infraestructura Tecnológica
- Diseño de las Planillas de Evaluación de la Seguridad General y Física
- Programación de trabajos con los Proveedores involucrados
- Verificación de las dependencias del CNC
- Trabajo de Campo
- Presentación del Objetivo y Alcance de la Evaluación y Concienciación en materia de Seguridad a los Responsables y Funcionarios
- Identificación de las vulnerabilidades en base a la situación encontrada en cada una de las dependencias del Área Técnica y alrededores del CNC.
- Análisis y Diagnóstico de la Situación Encontrada, descripción de los Puntos Críticos y Puntos a Mejorar.
- Elaboración del Mapeo General de la situación encontrada
- Reuniones de Trabajo con las Áreas Involucradas
- Confección de Gráficos demostrativos y comparativos de la Situación Actual.

# 4 Fase II: Formalización de Procesos de Seguridad de la Infraestructura de TI de ARANDU

Los Procesos de Seguridad de la información, salvaguardan tanto a la Red como a los usuarios frente a amenazas que pudieran detectarse, por ello, la formalización de los procesos permitió elaborar un plan orientado a mantener la continuidad del servicio.

En este ámbito, se aplicaron las buenas prácticas de la industria de TI con el propósito de proponer planes y estrategias concretas de optimización de los recursos y aumento de los niveles de calidad de los procesos.

Del mismo modo, dicho Plan debe ser evaluado y mejorado (si fuese necesario) periódicamente, alineándose a las necesidades organizativas de ARANDU.

El desarrollo de esta Fase fue enmarcado en los siguientes objetivos:

## 4.1 Objetivo General

Definir los delineamientos que direccionen y apoyen la seguridad de la infraestructura tecnológica de ARANDU.

## 4.2 Objetivos Específicos

- Elaborar las Políticas de Seguridad de TI
- Elaborar el Plan de Capacitación en temas relacionados a la Seguridad de la Infraestructura de TI

- Desarrollar la Jornada de Capacitación

### 4.3 Alcance de la Fase II

La seguridad de la información es una atribución inherente a todas las funciones y los cargos de ARANDU. En consecuencia, las políticas abarcan todo el ámbito de la Red y a los funcionarios que interactúan en las diferentes áreas de las instituciones miembros.

### 4.4 Metodología de Trabajo

Fue aplicado el Enfoque Metodológico abierto e internacionalmente aceptado CobiT®. Esta metodología permitió la evaluación de los Procesos, Actividades y Tareas de la Dirección General, el Área Técnica y el Taller de Soporte Técnico y Mantenimiento.

La aplicación de CobiT® facilitó la evaluación por medio de un benchmarking con las mejores prácticas del mercado, de forma a optimizar y alcanzar el nivel apropiado de gobernabilidad sobre la Seguridad de la Información administrada en ARANDU.

El enfoque está construido en base al Circulo Virtual de Calidad: Planificar + Diseñar + Ejecutar + Monitorear y abarca los siguientes Dominios:

- PLANIFICACION Y ORGANIZACION: Este dominio cubre las estrategias y las tácticas, e identifica la manera en que la TI pueda contribuir de la mejor forma al logro de los objetivos de la Infraestructura de TI de ARANDU. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una Estructura Organizacional y una Estructura Tecnológica apropiada.
- ADQUISICION E IMPLEMENTACION: Las Soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los Objetivos de la Infraestructura de TI de ARANDU.
- PRODUCCION Y SERVICIOS: Este dominio cubre la entrega de los servicios requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.
- MONITOREO Y EVALUACION: Todos los procesos de TI deben evaluarse de forma regular en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno y la seguridad, el cumplimiento regulatorio y la aplicación del Gobierno de TI.

**4.5 Tareas Realizadas**

Como resultado del reconocimiento de la Infraestructura Tecnológica de ARANDU administrada por el Área Técnica del Centro Nacional de Computación, de la Evaluación del Control Interno de la Seguridad de los Sistemas de Información, de la Identificación de los Procesos del Negocio que dependen de la Tecnología de Información y del relevamiento de la situación actual en materia de formalización de los Procesos, Actividades y Tareas involucradas en la Seguridad General de la Información, fueron desarrolladas las siguientes Políticas:

- SEGURIDAD DE LA INFORMACIÓN
  - Establecer las líneas maestras y los principios que direccionan y apoyan la seguridad de la información, que satisfaga los requerimientos institucionales de mantener la integridad de la información y minimizar el impacto de vulnerabilidades e incidentes de seguridad en la infraestructura tecnológica de ARANDU.
- CLASIFICACIÓN DE LA INFORMACIÓN
  - Orientar a los funcionarios en cuanto a la clasificación de la información de la Institución y al tratamiento adecuado de acuerdo con el nivel de confidencialidad.
- FUNCIONES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN
  - Asignar las funciones y responsabilidades referentes a la Seguridad de la Información a los Empleados.
- GESTIÓN DE ACTIVOS DE LA INFORMACIÓN
  - Fijar conceptos y orientar a los funcionaros en cuanto a la gestión de los activos de información de la infraestructura tecnológica de ARANDU.
- ADMINISTRACIÓN DE RECURSOS DE TI
  - Establecer las líneas maestras y los principios que direccionan y apoyan la utilización de los Recursos de TI (Hardware, Software, Servicios de Red) por los funcionarios de ARANDU.
- MESA LIMPIA
  - Disciplinar los criterios para minimizar el riesgo de exposición indebida e información confidencial en las dependencias de las Instituciones. Incluye medidas de seguridad en la custodia y eliminación de documentos y para la acción de inspección.
- SEGURIDAD EN LA UTILIZACIÓN DE LAS ESTACIONES DE TRABAJO
  - Definir Normas y estándares de seguridad en la utilización de las Estaciones de Trabajo.
- SEGURIDAD DE LAS COMUNICACIONES
  - Establecer las normas que garanticen la implementación de técnicas de seguridad y procedimientos para autorizar los accesos y controlar los flujos de información desde y hacia las redes de comunicaciones internas (Intranet) y las externas (Extranet e Internet).
- SEGURIDAD EN LA UTILIZACIÓN DEL CORREO ELECTRÓNICO
  - Orientar en la utilización de Correo Electrónico, por normas, patrones de seguridad y mejores prácticas.

- SEGURIDAD EN LA UTILIZACIÓN DE MEDIOS DIGITALES DE ALMACENAMIENTO
  - Reglamentar la utilización de medios digitales de almacenamiento por medio de normas y de estándares de seguridad.

El objetivo de la Jornada de Capacitación y Evaluación sobre la Seguridad de la Información, fue capacitar a los funcionarios asignados a la Gestión del Centro Operaciones de Red y de Puntos de Presencia acerca de los conceptos de Seguridad y las Políticas desarrolladas a fin de concienciar y asegurar la implementación de las mismas.

Los temas desarrollados durante la jornada fueron los siguientes:

- Marco de Referencia Internacional CobiT®
- Conceptos de Políticas, Normas, Procedimientos e Instructivos
- Principios de la Seguridad de la Información:
- Ciclo de Vida de la Información:
- Responsabilidades de los principales actores
- Tipos de Información
- Niveles de Confidencialidad de la Información
- Requisitos de Control y Protección
- Consejos Generales sobre Seguridad de la Información
- Propietario de la Información. Conceptos y Responsabilidades

# 5 Fase III: Garantía de Continuidad del Servicio

Un Plan de Continuidad de TI es un conjunto de tareas que ARANDU realizará en caso de fallas en la infraestructura, que impidan el normal funcionamiento de los servicios TI, a fin de recuperar en el menor tiempo posible las operaciones de la Red.

El enfoque para lograr la continuidad de los servicios TI de ARANDU apunta a medidas preventivas, que eviten la interrupción de los servicios y medidas reactivas, que recuperen los niveles aceptables de servicio en el menor tiempo posible.

Las actividades de prevención y recuperación deben ofrecer las garantías necesarias a costos razonables.

## 5.1 Objetivo General

Garantizar la continuidad de los servicios brindados por la infraestructura tecnológica de ARANDU ante interrupciones no planificadas.

## 5.2 Objetivos Específicos

- Desarrollar un marco de trabajo de continuidad de TI para soportar la secuencia de las operaciones de ARANDU, como un proceso consistente
- Determinar los recursos críticos de TI relacionados al Plan de Contingencia
- Elaborar el Plan de Pruebas del Plan de Contingencia de TI

- Confeccionar el Plan de Capacitación en el Plan de Contingencia de TI

### 5.3 Alcance de la Fase III

El desarrollo del Plan de Contingencia de TI fue diseñado para minimizar el impacto de una interrupción en las funciones y procesos clave del servicio brindado por ARANDU.

Para el efecto, el Marco de Trabajo de Continuidad de TI toma en cuenta la estructura organizacional para administrar la continuidad, la cobertura de los roles, las tareas y las responsabilidades del personal interno y externo, su administración y las instituciones usuarias. Asimismo, toma en cuenta las reglas y estructuras para documentar, probar y ejecutar los planes de contingencia de TI.

El plan considera puntos tales como la identificación de los Recursos Críticos de la Infraestructura de TI, el monitoreo y reporte de la disponibilidad de los recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

Centra la atención en los puntos determinados como los más críticos en el plan de contingencia de TI, para construir resistencia y establecer prioridades en situaciones de recuperación, asegura que la respuesta y la recuperación están alineadas con las necesidades prioritarias de ARANDU, asegurando también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales.

Para asegurar que el Plan de Contingencia de TI se mantenga actualizado y que refleje de manera continua los requerimientos de ARANDU, los miembros del Equipo Técnico tiene la responsabilidad de definir y ejecutar procedimientos de control de cambios que garanticen que dichos cambios y las responsabilidades sean comunicados de forma clara y oportuna.

El Plan de Continuidad de TI contempla la Infraestructura Tecnológica de Información del Centro de Operaciones de Red (NOC ï Network Operating Center), que debe operar 7 x 24 x 365, vigilando la red de alarmas o de condiciones que pueden requerir atención especial para mitigar el impacto en el servicio y rendimiento de la Red.

El Plan de Pruebas del Plan de Contingencia de TI tiene como objetivo probar el plan de forma regular para asegurar que la Infraestructura de TI de ARANDU puede ser recuperada en forma efectiva, que las deficiencias sean atendidas y que el plan permanece aplicable en el tiempo establecido.

### 5.4 Tareas Realizadas

Como resultado de los trabajos desarrollados para Garantizar la Continuidad de los Servicios, de la evaluación del control interno, de la identificación de los recursos críticos, servicios brindados, los roles y responsabilidades definidas para la gestión de ARANDU, fueron desarrollados los siguientes trabajos:

- MARCO DE TRABAJO DE CONTINUIDAD DE TI
  - Establecer un marco de trabajo de continuidad de TI para soportar las operaciones de la Red con un proceso consistente a lo largo de toda la

organización, que brinde la garantía suficiente que, ante la ocurrencia de una crisis, los servicios considerados críticos continúen operando o puedan ser recuperados en un tiempo adecuado.

- INFORME DE LOS RECURSOS CRÍTICOS DE LA INFRAESTRUCTUERA DE TI
  - Centrar la atención en los puntos determinados como los más críticos en el plan de contingencia de TI.
- PLAN DE CONTINGENCIA DE LA INFRAESTRUCTURA DE TI DE ARANDU
  - Establecer un Plan de Contingencia de TI que será utilizado como referencia principal en caso de ocurrencia de una situación que interrumpa la normal operatoria de los procesos críticos.
- PLAN DE PRUEBAS DEL PLAN DE CONTINGENCIA DE TI
  - Establecer un procedimiento para la realización de las pruebas de contingencia de la infraestructura tecnológica de ARANDU, que garantice la realización y documentación adecuada de cada una de las pruebas.

# 6 Fase IV: Entrenamiento

La capacitación fue planeada de forma estructurada y coherente con las exigencias de recuperación de la operativa normal de ARANDU.

El plan anual de capacitación para la realización de pruebas de contingencia contempla acciones de capacitación que nacen a partir de tres grandes fuentes:

- Las necesidades de mejoramiento de la gestión que garantizan la continuidad del negocio
  - Acciones de capacitación que apoyarán el logro de los objetivos de gestión relacionados con los sistemas y equipos críticos que necesitan un ambiente de contingencia
- El ámbito del Marco de Referencia Internacional CobiT®, en el Objetivo de Control de Alto Nivel PS2[5], en el punto PS2.4 recomienda entrenar regularmente a los participantes del plan respecto a pasos a seguir en caso de desastres o incidentes.
- El desarrollo institucional de ARANDU destinado principalmente al perfeccionamiento y/o desarrollo de competencias que permitan a la institución lograr sus objetivos y la entrega correcta de servicios.

## 6.1 Objetivo General

Garantizar que todas los integrantes del Equipo Técnico y funcionarios de ARANDU reciban sesiones de capacitación de forma regular respecto a los procesos, los roles y las responsabilidades de cada miembro en caso de la ocurrencia de un incidente.

[5] Garantizar la Continuidad del Servicio

### 6.2 Alcance de la Fase IV

Toda la Infraestructura de TI que soporta los servicios y procesos de negocio de las diferentes áreas de ARANDU.

Fueron identificados los servicios administrados por el área de Coordinación Técnica de la Red y catalogados como Críticos y Necesarios.

Todos los sistemas y equipos están contemplados en el Plan de Continuidad del Negocio de cada área.

Las jornadas de capacitación deben ser continuas y desarrollarse de manera exhaustiva para que todos los miembros estén familiarizados con todos los aspectos del proceso de recuperación, cubriendo todas sus facetas.

### 6.3 Entrenamiento en la ejecución del Plan de Contingencia

El Programa de Entrenamiento ha sido desarrollado para familiarizar al personal de ARANDU con el Plan de Contingencia en caso que se produzca una contingencia en la provisión de servicios.

- El Equipo de recuperación de desastres recibirá una comprensión total de las acciones a tomar para responder a los eventos que se presenten, los tiempos y aspectos técnicos de sus respectivas tareas de recuperación.

La metodología consiste en presentar una visión general del Plan de Contingencia con la intención de establecer la capacidad de reacción del personal técnico y administrativo para llevar a cabo las tareas que le son asignadas.

Estas jornadas también permiten:

- Identificar al funcionario idóneo en un servicio crítico, para convertirse en capacitador oficial y líder del equipo de recuperación en dicho servicio
- Identificar los funcionarios ñbackupò del líder del equipo de recuperación
- Comprender el procedimiento de pruebas de contingencia
- Comprender cada una de las actividades del Plan de Contingencia para cada servicio crítico y escenario de desastre
- Detallar los recursos críticos a ser utilizados y los proveedores externos involucrados en situación de contingencia
- Crear unidad entre los miembros del equipo de recuperación

El método didáctico utilizado durante las sesiones de entrenamiento fue el método de discusión, teniendo en cuenta los siguientes aspectos:

- Informar sobre los objetivos, importancia y la estructura del Plan de Contingencia
- Entrenar en la realización de las pruebas de contingencia de los servicios
- Entrenar en el uso de sistemas o equipos en momentos de emergencia, para cada escenario.
- Aumentar el grado de concienciación ante un desastre y asegurar su apoyo en el proceso de recuperación de las operaciones críticas.

#### 6.4. Programa del Entrenamiento

El contenido desarrollado fue el siguiente:

1. Objetivos, importancia y estructura del Plan de Contingencia de TI

2. Diferencia entre Plan de Continuidad del Negocio (BCP ï Business Continuity Planning) y Plan de Contingencia de TI (DRP ï Disaster Recovery Planning)
3. Procesos de Negocios, Servicios Críticos, Sistemas Aplicativos y Plataformas relacionadas
4. Recursos Críticos de la Infraestructura de TI
5. Selección de Estrategias de Recuperación
6. Requerimientos mínimos para procesos críticos y necesarios
7. Conformación del Equipo de Recuperación, Funciones Principales
8. Mantenimiento del Plan, Administración de Cambios
9. Pruebas del Plan de Contingencia de TI
10. Entrenamiento respecto al Plan de Contingencia de TI
11. Sitio de Contingencia
12. Escenarios, Amenazas, Estrategias
13. Descripción de los procesos de recuperación
14. Contactos de Emergencia
15. Estructura de Decisión

# 7 Fase V: Evaluación de la Implementación

La evaluación de la implementación permite probar que los planes de contingencia son capaces de proporcionar el nivel deseado de soporte de los principales procesos del negocio, permitiendo validar que el plan puede llevarse a cabo dentro de un período de tiempo dado, proporcionando la oportunidad de hacer los ajustes necesarios al plan y al ambiente dentro del cual es probado.

Finalmente, la prueba permite la oportunidad para una valoración detallada del costo de operación bajo una contingencia y la idoneidad de los líderes de recuperación de los servicios.

## 7.1 Objetivo General

Asegurar que las Políticas, Normas y Procedimientos de Seguridad de TI y el Plan de Continuidad de TI se mantengan actualizados y que refleje de manera continua los requerimientos actuales de la Infraestructura de TI de ARANDU.

## 7.2 Tareas Realizadas

- Relevamiento de la implementación de la Seguridad de la Infraestructura de TI
- Evaluación el grado de implementación y cumplimiento de las normativas definidas
- Identificación de nuevos requerimientos
- Realización de la retroalimentación de Políticas, Normas y Procedimientos de Seguridad de TI y el Plan de Continuidad de TI
- Elaboración del Informe de Recomendaciones para adecuaciones necesarias

## 8 Conclusión

Contar con un Plan de Continuidad significa para ARANDU que está preparada adecuadamente para enfrentar cualquier eventualidad, garantizando la provisión de servicios, salvaguardando los intereses de sus miembros, su reputación y las actividades creadoras de valor.

Es de gran importancia la planificación de jornadas de capacitación continua y desarrollarse de manera exhaustiva para que todos los miembros estén familiarizados con todos los aspectos del proceso de recuperación.

Gracias al Plan de Continuidad del Negocio, independiente de la causa del incidente que genera una interrupción, ARANDU pondrá en funcionamiento una estructura de respuesta ante incidentes garantizando a los usuarios de sus servicios la recuperación de la operatividad de la Red en el menor tiempo posible.

## 9 Agradecimientos

Los autores agradecen la colaboración del Ing. Vicente Clemotte, Consultor principal para la elaboración del Plan de Continuidad del Negocio de ARANDU.