Documento "f" Proyectos o Propuestas del Plan de Recuperación de Desastres y del Plan de Continuidad de Negocios

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Documento "f"

Presentar los Proyectos o Propuestas del Plan de Recuperación de Desastres y del Plan de Continuidad de Negocios en el ámbito de su competencia.

"Centro de Productividad Avanzada S.A. de C.V." (en lo sucesivo CEPRA)
"Términos de Referencia y Apéndices" (en lo sucesivo ANEXO 1)
"Puestos de Servicio (en lo sucesivo PS)"

1.- Beneficios (Sección 1.2 del ANEXO 1)

El objetivo de este documento es que CEPRA provea servicios de forma asociada a los niveles de servicio que garanticen la continuidad de la operación del Servicio de Administración Tributaria (SAT), así como el aseguramiento de su calidad y oportunidad.

2.- Responsabilidad (Sección 1.3 del ANEXO 1)

Con base en este documento y en lo requerido sucesivamente por el cliente, CEPRA preservará en todo momento y circunstancia la continuidad operativa de los servicios que prestarán los PS, además, apoyará en la recuperación de dicha continuidad, como resultado de desastres naturales o cualquier otra eventualidad ajena al SAT.

3.- Planeación del arranque (Sección 2.3.1 del ANEXO 1)

CEPRA entiende y se compromete a participar de forma activa en el desarrollo de la definición del alcance y la realización del futuro Plan de Continuidad de Negocio (BCP), Plan de Recuperación de Desastres (DRP) y el Plan de Anticipación a Fenómenos Naturales (AFN) de la Institución, aplicable en el ámbito de la competencia de CEPRA.

4.- Entregables de la Planeación del arranque (Sección 2.3.1.1 del ANEXO 1)

Como parte de la fase de planeación del arranque, CEPRA se compromete a entregar la definición del alcance, pruebas y demás que se deban desempeñar respecto del BCP, DRP y AFN del SAT, formalizado y firmado por el Cuerpo de Gobierno y CEPRA.

5.- Documentación del servicio (Sección 4.2.1.7 del ANEXO 1)

CEPRA entregará a la Administración de Infraestructura Externa de manera periódica los resultados de las pruebas del Plan de Continuidad de Negocio (BCP) y del Plan de Recuperación de Desastres (DRP), estos serán expresados como reportes que muestren los resultados de dichas pruebas del BCP o DRP y las acciones realizadas en caso de ejecutar dichos planes cuando aplique. Estos reportes serán entregados conforme a los acuerdos establecidos con el SAT durante las mesas de planeación ó cuando sea requerido.

6.- Acuerdos de nivel de operación (Sección 5.1 del ANEXO 1)

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

CEPRA será responsable de asegurar la continuidad en la operación del equipo de cómputo, dispositivos especializados y accesorios adicionales que estén bajo su servicio, incluyendo las piezas y refacciones, para cumplir con los SLA´s establecidos.

CEPRA solucionará las contingencias que se presenten en los componentes que integran los diversos servicios que presta con el objeto de mantenerlos en operación de manera continua.

CEPRA participará en las actividades programadas de común acuerdo con el SAT que permitan identificar la correcta aplicación de un futuro Plan de Continuidad de Negocio (BCP) y un Plan de Recuperación de Desastres (DRP), así como el Plan de Anticipación a Fenómenos Naturales (AFN). CEPRA está consciente de que el detalle de las actividades en las que debe involucrarse se definirá en la Fase de Planeación del arranque del proyecto.

Introducción

El presente documento tiene por objeto presentar los proyectos del Plan de Recuperación de Desastres y del Plan de Continuidad de Negocios de CEPRA. Este documento incluye también el Plan de Anticipación de Fenómenos Naturales.

DISTRIBUCION:
Área infraestructura, directores de departamento, gerencia infraestructura, y / o a quien lo solicite).

a)Nombre
FUNDAMENTO LEGAL: Artículo 3 fracción II, 18 fracciones I y II, y 19 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el segundo párrafo del Segundo Transitorio y primer párrafo del Cuarto Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública publicada en el Diario oficial de la Federación el 09 de mayo de 2016, así como en el Lineamiento Trigésimo Octavo, Trigésimo noveno y Cuadragésimo, de los Lineamientos Generales para la Clasificación y Desclasificación de la información de las dependencias y entidades de la Administración Pública Federal publicado en el mismo órgano de difusión el 15 de abril de 2016.
Motivación: Datos personales y/o datos financieros y/o patrimonial

TABLA DE CONTENIDO

HISTORIA DE ENMIENDAS

Cuando este documento sea modificado, llenar la columna de enmiendas y brevemente describir los cambios hechos en un párrafo corto.

LAS FIRMAS DE APROBACION ESTAN DISPONIBLES EN EL ARCHIVO DE COPIA MAESTRA

# REV	ESCRITO POR	APROBADO POR	FECHA	SECCION (ES)	ENMIENDAS
01	a) Eliminado		27/05/09	NA	NA

Espacio intencionalmente en blanco

ÍNDICE GENERAL

Contenido

Plan de Continuidad del Negocio

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

INTRODUCCIÓN

El plan de continuidad del negocio es una estrategia constituida por un conjunto de procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los procesos de negocio afectados por una paralización total o parcial de la capacidad operativa.

El diseño del BCP involucra grandes consideraciones de planeación. Existen generalmente tres áreas de acción a la que está dirigido:

- Pérdida de la capacidad de comunicación, como: voz y datos.
- Pérdida de la capacidad de procesamiento.
- Pérdida del espacio de trabajo.

La responsabilidad de llevar a cabo esta planeación dentro de las áreas de negocio deberá ser asumida por todas las áreas de negocio, sin embargo la planeación de contingencia debe ser coordinada por el área de infraestructura de CEPRA

Para desarrollar el plan de continuidad del negocio, deben entenderse las diferentes fases de un desastre. El ciclo de vida de un desastre consta de cuatro periodos de tiempo:

1. Operaciones normales. Las operaciones normales indican el periodo de tiempo antes de que ocurra un desastre. Esta fase del plan debe incluir la práctica de las operaciones que pretenden prevenir un desastre desde que principia, y de aquellas que ayudan a mitigar el impacto del mismo.

2. Respuestas de emergencia. Las respuestas derivadas de una situación de emergencia ocurren durante las pocas horas que siguen inmediatamente a un desastre. Esta fase de un plan identifica las actividades que pueden necesitar mayor atención durante este periodo, con la finalidad de asegurar una respuesta a CEPRA y proporcionar una lista de verificación de las actividades importantes que pueden pasar inadvertidas durante la confusión que acompaña a los desastres.

3. Procesamiento interno. El procesamiento interno es un procedimiento alternativo que representa el tiempo de duración de la contingencia en relación con el soporte de las funciones esenciales de CEPRA hasta que la capacidad de procesamiento normal sea restaurada.

4. Restauración. Se debe también indicar el periodo de tiempo destinado a aquellas actividades que se necesita realizar para recuperar una condición o capacidad de procesamiento en su operación normal. La restauración involucra necesariamente los pasos de la planeación, organización y control de tales actividades.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Este plan incluye los documentos clave los cuales abordan temas de la prevención de desastres, actividades para proporcionar una respuesta inmediata, procedimientos de recuperación o salvamento y de rehabilitación de materiales dañados.

Este plan no es limitativo, por tal motivo cuando así lo determinen las necesidades o requerimientos del negocio, se podrán adicionar planes, procedimientos, formatos y cualquier otro documento que así se requiera.

OBJETIVO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

El objetivo del Plan de Continuidad del Negocio (BCP) es describir las actividades que deben ser realizadas en toda la organización, para mantener la operación del proceso de negocio en caso de desastre.

Este plan contiene los siguientes documentos:

- Análisis de riesgos. Su contenido permite identificar aquellos eventos más comunes que pueden ocasionar interrupciones en los procesos de negocio de CEPRA, junto con la probabilidad y el impacto de dichas interrupciones.

- Declaratoria de aplicabilidad. Documento que menciona la adopción de controles del estándar ISO/IEC 27001:2005 por pate de CEPRA para el tratamiento de los riesgos descritos en el Análisis de Riesgos.

- Metodología para la elaboración del plan de continuidad y disponibilidad. Describe la secuencia de actividades que deben realizarse para la elaboración, aprobación y revisión de los planes de disponibilidad y continuidad del negocio.

- Plan de recuperación de desastres (DRP). Menciona las actividades necesarias a realizar para la recuperación de los servicios de TI en caso de una interrupción ocasionada por una contingencia o desastre; dentro de este documento se incluyen planes de contingencia para la recuperación de los subsistemas que soportan la infraestructura de los servicios que se proporcionan.

- Plan de anticipación de fenómenos naturales (AFN). Describe las actividades que CEPRA desarrolla para la anticipación y respuesta ante la manifestación de fenómenos naturales que pongan en riesgo la integridad del recurso humano y/o la integridad de la infraestructura de la organización.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

ALCANCE

Este plan de continuidad del negocio tiene amplitud sobre las operaciones vitales de CEPRA, abarca las áreas que la integran y las principales actividades que en ellas se desarrollan.

Durante la fase de planeación de arranque, el Plan de Continuidad del Negocio estará alineado a las políticas de continuidad y recuperación que el proyecto de APS requiera, esto conforme a lo expuesto en la sección 5.8 del Documento 1 de esta propuesta técnica.

ESCENARIOS

Los posibles escenarios ante los cuales se activa el presente plan de continuidad del negocio están en función del nivel de severidad del evento presentado, el siguiente cuadro muestra las situaciones posibles:

Nivel de severidad	Características
Interrupción	➢ No hay modificación en la carga de trabajo programada de las funciones y operaciones no afectadas. ➢ Solo es necesaria poca movilización de los elementos del plan de continuidad del negocio. ➢ Ejemplos de una interrupción pueden incluir: o Problemas de red. o Breve Interrupción de energía.
Contingencia	➢ Puede ser necesaria la activación parcial del plan de continuidad para responder y corregir el problema identificado. ➢ Ejemplos de una contingencia pueden incluir: o Pérdida total de las comunicaciones. o Falla en el aire acondicionado en centros de procesamiento de información. o Inundaciones o Fuego controlable. o Daños moderados a la instalación de la red pública-privada.
Desastre	➢ Se estima que la interrupción será mayor que el tiempo de recuperación en caso de falla ➢ Las instalaciones primarias podrán no estar disponibles por lo que una localidad secundaria puede empezar a servir como primaria. ➢ Debe iniciarse el envío de tecnología de respaldo desde el almacén externo. ➢ Se ordena la activación total del plan de continuidad. ➢ Ejemplos de un desastre pueden incluir: o Fuego fuera de control o Interrupción prolongada y masiva de telecomunicaciones o Terremotos, etc.

ANÁLISIS DE RIESGOS

Introducción

Numerosas operaciones comerciales se han visto frustradas por robo de información, fenómenos ambientales adversos, guerras, disturbios o daños accidentales. Adicionalmente existen otra serie de riesgos que tienen que ver con temas como la privacidad, la seguridad el terrorismo o malas prácticas ejecutivas.

Actualmente las organizaciones modernas dependen en gran medida de la Tecnología de la Información, no sólo desde el punto de vista operacional, sino también para gestionar y aprovechar la información con propósitos competitivos. Por ello el riesgo relacionado con la TI es un hito a tener en cuenta en el actual entorno empresarial.

Se define al riesgo como una función de la probabilidad de que un cierto peligro o amenaza ocurra y la magnitud de sus consecuencias.

El análisis de riesgo es una metodología que sirve para identificar y evaluar probables daños y pérdidas a consecuencia del impacto de una amenaza sobre grupos de personas, comunidades y municipios.

[*Adicionalmente implica un análisis de las amenazas y un análisis de la vulnerabilidad (probabilidad de ocurrencia) y deben entenderse como actividades inseparables; es decir no se puede hacer un análisis de los factores naturales y socionaturales (amenazas) sin conocer las debilidades (vulnerabilidades) de los grupos sociales.*]

Objetivo

1. Identifica, analiza y documenta de manera participativa las posibles amenazas naturales y socio-naturales.
2. Cuantificar la vulnerabilidad y darle un valor para lo cual se obtiene un promedio de los valores de exposición, fragilidad y resistencia.
3. Descubrir y planificar las medidas oportunas para mitigar y mantener los riesgos bajo control.

Aplicación del Análisis de Riesgos

Describir el enfoque del análisis de riesgos y los procesos, áreas y/o servicios que se encuentran en el alcance del documento.

Se contempla el análisis de riesgos de los siguientes servicios:

a) Mesa de Servicios
b) Call Center Especializado
c) NOC (Network Operations Center)

Análisis de Riesgos

Estimación del Riesgo

La estimación del riesgo se realizó mediante un esquema de matrices, En la estimación del riesgo se asume valores para la probabilidad de ocurrencia del evento analizado y se determina la potencial severidad de las consecuencias que podría ocasionar dicho evento.

A continuación se describe la metodología seguida para la estimación del riesgo, en donde se definen la probabilidad de ocurrencia y la severidad del daño que cualquier evento que se quiera analizar.

Para el caso de los servicios listados anteriormente, se plantearon matrices de estimación de riesgos asociadas con los siguientes eventos:

- Gente e Instalaciones
- Sistemas de TI, redes y procesos
- Servicios críticos (energía, agua, teléfono, etc.)
- Activos críticos (contratos, garantías, etc.)

Estos eventos se pueden generar por factores externos, como terremotos, altas precipitaciones, ámbito político, social, económico, etc.

Probabilidad de Ocurrencia

Para este análisis, la probabilidad de ocurrencia se considera como la posibilidad de que un evento ocurra durante el ciclo de vida de cada unos de los servicios considerados.

1. **No se espera que ocurra durante el ciclo de vida del proyecto y/o servicio.**
2. **Se espera que ocurran no más de una vez durante la vida del proyecto y/o servicio.**
3. **Se espera ocurra varias veces durante la vida del proyecto y/o servicio.**
4. **Se espera ocurra más de una vez al año.**

Severidad de las Consecuencias

Se califica adoptando una cuantificación de la afectación al negocio y a la infraestructura, resultado del evento evaluado.

1	**Negocio del cliente**	El negocio tiene una pérdida mínima o nula de recursos financieros.
	Imagen de CEPRA	Mínima o nula imagen negativa en la percepción del cliente hacia los servicios de CEPRA.
	Penalizaciones	Perdida mínima o nula de recursos financieros de CEPRA.
	Daño a la Infraestructura	Mínima o nulo daño a la infraestructura de CEPRA.

2	**Negocio del cliente**	El negocio tiene una pérdida mesurada de recursos financieros.
	Imagen de CEPRA	Imagen negativa mesurada en la percepción del cliente hacia los servicios de CEPRA.
	Penalizaciones	Perdida mesurada de recursos financieros de CEPRA.
	Daño a la Infraestructura	Daño mesurado en la infraestructura de CEPRA.

3	**Negocio del cliente**	El negocio tiene una pérdida considerable de recursos financieros.
	Imagen de CEPRA	Imagen negativa considerable en la percepción del cliente hacia los servicios de CEPRA.
	Penalizaciones	Pérdida considerable de recursos financieros de CEPRA.
	Daño a la Infraestructura	Daño considerable en la infraestructura de CEPRA.

4	**Negocio del cliente**	El negocio tiene una pérdida crítica de recursos financieros.
	Imagen de CEPRA	Imagen negativa crítica en la percepción del cliente hacia los servicios de CEPRA.
	Penalizaciones	Perdida crítica de recursos financieros de CEPRA.
	Daño a la Infraestructura	Daño crítico en la infraestructura de CEPRA.

Resultado de la Evaluación de Riesgos

Una vez comparados los resultados de la probabilidad de ocurrencia versus la severidad de las consecuencias para cada evento evaluado, la evaluación del riesgo provee, la importancia de cada evento analizado, mediante la aplicación de los valores establecidos en la tabla 2. La tabla 1 presenta la escala de jerarquía del riesgo.

TABLA 1
CATEGORÍA DE IMPORTANCIA DEL RIESGO

NÚMERO	CATEGORÍA	DESCRIPCIÓN
I	Inaceptable	El riesgo debe ser reducido o si es posible eliminarlo inmediatamente. Situaciones donde los esfuerzos de recuperación son muy difíciles. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III o IV.
II	Indeseable	Implementación de planes de contingencia para evitar la interrupción de los servicios de la Mesa. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III.
III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.

TABLA 2
MATRIZ DE EVALUACIÓN DE RIESGOS

PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4
1	**IV**	**IV**	**IV**	**III**
2	**IV**	**IV**	**III**	**II**
3	**IV**	**III**	**II**	**I**
4	**III**	**II**	**I**	**I**

Con los resultados obtenidos en la tabla 2, se procede a asignar jerarquía a los eventos analizados, seguidas de una descripción de las acciones a tomar.

Estas acciones servirán de guía para la elaboración de un plan de contingencia que formará parte del "Plan de Continuidad de CEPRA".

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

SERVICIO: MESA DE SERVICIOS

Evaluación de Riesgos: GENTE E INSTALACIONES

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Ausentismo del total de los Agentes de la Mesa de Servicios (enfermedad, incapacidad, accidente, etc.)	X						X	
Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)		X					X	
Incendio en las instalaciones.	X						X	
Sismo catastrófico.				X				X
Inundación catastrófica.		X					X	

Resultados de Estimación de Riesgo: GENTE E INSTALACIONES

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Ausentismo del total de los Agentes de la Mesa de Servicios (enfermedad, incapacidad, accidente, etc.)	1	3	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Incendio en las instalaciones.	1	3	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Sismo catastrófico.	4	4	I	Inaceptable	El riesgo debe ser reducido o si es posible eliminarlo inmediatamente. Situaciones donde los esfuerzos de recuperación son muy difíciles. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III o IV.
Inundación catastrófica.	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.

Evaluación de Riesgos: SISTEMAS DE TI, REDES Y PROCESOS

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Inoperatividad de las redes de voz y datos dentro del Site de la Mesa de Servicios			X				X	
Daños en servidores de aplicación y de la base de datos		X					X	
Falla en los equipos (estaciones de trabajo)			X			X		
Falla en el servicio de internet		X				X		

Resultados de Estimación de Riesgo: SISTEMAS DE TI, REDES Y PROCESOS

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUE|NCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Inoperatividad de las redes de voz y datos dentro del Site de la Mesa de Servicios	3	3	II	Indeseable	Implementación de planes de contingencia para evitar la interrupción de los servicios de la Mesa. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III.
Daños en servidores de aplicación y de la base de datos	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falla en los equipos (estaciones de trabajo)	3	2	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falla en el servicio de internet	2	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Evaluación de Riesgos: SERVICIOS CRÍTICOS (ENERGÍA, AGUA, TELÉFONO, ETC)

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Fallas de energía eléctrica.			X					X
Fallas del sistema telefónico.		X					X	
Falta de iluminación	X				X			
Falta de agua	X				X			
Fallas en el sistema de enfriamiento		X					X	
Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)		X					X	

Resultados de Estimación de Riesgo: SERVICIOS CRÍTICOS (ENERGÍA, AGUA, TELÉFONO, ETC)

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Fallas de energía eléctrica.	3	4	I	Inaceptable	El riesgo debe ser reducido o si es posible eliminarlo inmediatamente. Situaciones donde los esfuerzos de recuperación son muy difíciles. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III o IV.
Fallas del sistema telefónico.	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falta de iluminación	1	1	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Falta de agua	1	1	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Fallas en el sistema de enfriamiento	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.

Evaluación de Riesgos: ACTIVOS CRÍTICOS (CONTRATOS, GARANTÍAS, ETC.)

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Pérdidas de contratos y/o SLA's	X					X		
Pérdida de Procedimientos documentados	X					X		

Resultados de Estimación de Riesgo: ACTIVOS CRÍTICOS (CONTRATOS, GARANTÍAS, ETC.)

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Pérdidas de contratos y/o SLA's	1	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Pérdida de Procedimientos documentados	1	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.

Resultado del análisis de riesgos

El análisis de riesgo efectuado nos arroja que los eventos con menos probabilidad de ocurrencia son:

- Ausentismo del total de los Agentes de la Mesa de Servicios (enfermedad, incapacidad, accidente, etc.)
- Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)
- Incendio en las instalaciones.
- Inundación catastrófica.
- Inoperatividad de las redes de voz y datos dentro del Site del NOC
- Daños en servidores de aplicación de monitoreo y administración
- Falla en el servicio de internet
- Falta de iluminación
- Falta de agua
- Fallas en el sistema de enfriamiento
- Pérdidas de contratos y/o SLA's
- Pérdida de procedimientos documentados

Por otra parte, los eventos que representarían mayor pérdida financiera tanto para el negocio del cliente como de la Mesa de Servicios serían:

- Sismo catastrófico.
- Inoperatividad de las redes de voz y datos dentro del Site de la Mesa de Servicios
- Fallas de energía eléctrica.

Del mismo modo, existen eventos que requieren la implementación de controles para mitigar su impacto negativo como son:

- Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)
- Inundación catastrófica.
- Daños en servidores de aplicación y de la base de datos
- Falla en los equipos (estaciones de trabajo)
- Fallas del sistema telefónico.
- Fallas en el sistema de enfriamiento
- Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)

El resultado arroja que son 10 eventos que requieren atender inmediatamente para evitar pérdidas que van de lo considerado a lo crítico en cuento al negocio, imagen de la Mesa de Servicios, penalizaciones y daño a la infraestructura se refieren.

Las opciones de tratamiento más convenientes para cada evento se describirán en un documento anexo a este análisis de riesgos, donde se identificarán una gama de opciones de tratamiento de riesgos y su posterior implementación.

Las opciones de tratamiento que se enuncian a continuación no son limitativas ni serán apropiadas en todas las circunstancias.

EVITAR el riesgo. Se decide donde sea práctico, no proceder con servicios, procesos y/o actividades que podrían generar riesgos inaceptables, buscando con ello eludir el riesgo inherente asociado.

REDUCIR el riesgo. Se decide prevenir y/o reducir el riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al nivel más bajo posible, el cual debe ser compatible con las actividades de la Mesa de Servicios. Se puede conseguir con la optimización de los procedimientos y la implementación de controles.

REDUCIR la probabilidad de ocurrencia. Prevención del riesgo a través de la implementación de acciones tendientes a controlar su frecuencia o probabilidad.

REDUCIR las consecuencias o **MITIGAR** el riesgo. Reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si este sucede.

ATOMIZAR el riesgo. La Mesa de Servicios puede segmentar "el objeto" sobre la cual recae la amenaza de riesgo o distribuir la localización de "los objetos".

TRANSFERIR el riesgo. La Mesa de Servicios puede decidir traspasar o trasladar riesgos a otra parte o lugar de manera total o parcial. Las trasferencias parciales son conocidas como COMPARTIR el riesgo. La localización o distribución del riesgo en diversos lugares se conoce como DISPERSIÓN o ATOMIZACIÓN del riesgo.

ASUMIR el riesgo. La Mesa de Servicios decide aceptar los riesgos como ellos existen en la actualidad y establece políticas y estrategias financieras apropiadas para su tratamiento. En este caso la Mesa de Servicios considera que el riesgo residual actual es de bajo nivel y decide convivir con él, aceptando la pérdida probable, con la cual las estrategias de prevención se vuelven esenciales.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

SERVICIO: CALL CENTER ESPECIALIZADO

Evaluación de Riesgos: GENTE E INSTALACIONES

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Ausentismo del total de los Agentes de la Mesa de Servicios (enfermedad, incapacidad, accidente, etc.)	X						X	
Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)		X					X	
Incendio en las instalaciones.	X						X	
Sismo catastrófico.				X				X
Inundación catastrófica.		X					X	

Resultados de Estimación de Riesgo: GENTE E INSTALACIONES

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Ausentismo del total de los Agentes de la Mesa de Servicios (enfermedad, incapacidad, accidente, etc.)	1	3	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Incendio en las instalaciones.	1	3	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Sismo catastrófico.	4	4	I	Inaceptable	El riesgo debe ser reducido o si es posible eliminarlo inmediatamente. Situaciones donde los esfuerzos de recuperación son muy difíciles. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III o IV.
Inundación catastrófica.	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Evaluación de Riesgos: SISTEMAS DE TI, REDES Y PROCESOS

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Inoperatividad de las redes de voz y datos dentro del Site de la Mesa de Servicios			X				X	
Daños en servidores de aplicación y de la base de datos		X		s			X	
Falla en los equipos (estaciones de trabajo)			X			X		
Falla en el servicio de internet		X				X		

Resultados de Estimación de Riesgo: SISTEMAS DE TI, REDES Y PROCESOS

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUE|NCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Inoperatividad de las redes de voz y datos dentro del Site de la Mesa de Servicios	3	3	II	Indeseable	Implementación de planes de contingencia para evitar la interrupción de los servicios de la Mesa. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III.
Daños en servidores de aplicación y de la base de datos	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falla en los equipos (estaciones de trabajo)	3	2	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falla en el servicio de internet	2	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Evaluación de Riesgos: SERVICIOS CRÍTICOS (ENERGÍA, AGUA, TELÉFONO, ETC)

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Fallas de energía eléctrica.			X					X
Fallas del sistema telefónico.		X					X	
Falta de iluminación	X				X			
Falta de Agua	X				X			
Fallas en el sistema de enfriamiento		X					X	
Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)		X					X	

Resultados de Estimación de Riesgo: SERVICIOS CRÍTICOS (ENERGÍA, AGUA, TELÉFONO, ETC)

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Fallas de energía eléctrica.	3	4	I	Inaceptable	El riesgo debe ser reducido o si es posible eliminarlo inmediatamente. Situaciones donde los esfuerzos de recuperación son muy difíciles. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III o IV.
Fallas del sistema telefónico.	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falta de iluminación	1	1	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Falta de Agua	1	1	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Fallas en el sistema de enfriamiento	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Evaluación de Riesgos: ACTIVOS CRÍTICOS (CONTRATOS, GARANTÍAS, ETC.)

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Pérdidas de contratos y/o SLA's	X					X		
Pérdida de Procedimientos documentados	X					X		

Resultados de Estimación de Riesgo: ACTIVOS CRÍTICOS (CONTRATOS, GARANTÍAS, ETC.)

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Pérdidas de contratos y/o SLA's	1	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Pérdida de Procedimientos documentados	1	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.

Resultado del análisis de riesgos

El análisis de riesgo efectuado nos arroja que los eventos con menos probabilidad de ocurrencia son:

- Ausentismo del total de los Agentes del CALL CENTER Especializado (enfermedad, incapacidad, accidente, etc.)
- Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)
- Incendio en las instalaciones.
- Inundación catastrófica.
- Inoperatividad de las redes de voz y datos dentro del Site del NOC
- Daños en servidores de aplicación de monitoreo y administración
- Falla en el servicio de internet
- Falta de iluminación
- Falta de Agua
- Fallas en el sistema de enfriamiento
- Pérdidas de contratos y/o SLA's
- Pérdida de Procedimientos documentados

Por otra parte, los eventos que representarían mayor pérdida financiera tanto para el negocio del cliente como del CALL CENTER Especializado serían:

- Sismo catastrófico.
- Inoperatividad de las redes de voz y datos dentro del Site de la Mesa de Servicios
- Fallas de energía eléctrica.

Del mismo modo, existen eventos que requieren la implementación de controles para mitigar su impacto negativo como son:

- Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)
- Inundación catastrófica.
- Daños en servidores de aplicación y de la base de datos
- Falla en los equipos (estaciones de trabajo)
- Fallas del sistema telefónico.
- Fallas en el sistema de enfriamiento
- Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)

El resultado arroja que son 10 eventos que requieren atender inmediatamente para evitar pérdidas que van de lo considerado a lo crítico en cuento al negocio, imagen del CALL CENTER Especializado, penalizaciones y daño a la infraestructura se refieren.

Las opciones de tratamiento más convenientes para cada evento se describirán en un documento anexo a este análisis de riesgos, donde se identificarán una gama de opciones de tratamiento de riesgos y su posterior implementación.

Las opciones de tratamiento que se enuncian a continuación no son limitativas ni serán apropiadas en todas las circunstancias.

EVITAR el riesgo. Se decide donde sea práctico, no proceder con servicios, procesos y/o actividades que podrían generar riesgos inaceptables, buscando con ello eludir el riesgo inherente asociado.

REDUCIR el riesgo. Se decide prevenir y/o reducir el riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al nivel más bajo posible, el cual debe ser compatible con las actividades del CALL CENTER Especializado. Se puede conseguir con la optimización de los procedimientos y la implementación de controles.

REDUCIR la probabilidad de ocurrencia. Prevención del riesgo a través de la implementación de acciones tendientes a controlar su frecuencia o probabilidad.

REDUCIR las consecuencias o **MITIGAR** el riesgo. Reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si este sucede.

ATOMIZAR el riesgo. El CALL CENTER Especializado puede segmentar "el objeto" sobre la cual recae la amenaza de riesgo o distribuir la localización de "los objetos".

TRANSFERIR el riesgo. El CALL CENTER Especializado puede decidir traspasar o trasladar riesgos a otra parte o lugar de manera total o parcial. Las trasferencias parciales son conocidas como COMPARTIR el riesgo. La localización o distribución del riesgo en diversos lugares se conoce como DISPERSIÓN o ATOMIZACIÓN del riesgo.

ASUMIR el riesgo. El CALL CENTER Especializado decide aceptar los riesgos como ellos existen en la actualidad y establece políticas y estrategias financieras apropiadas para su tratamiento. En este caso el CALL CENTER Especializado considera que el riesgo residual actual es de bajo nivel y decide convivir con él, aceptando la pérdida probable, con la cual las estrategias de prevención se vuelven esenciales.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

SERVICIO: NOC (NETWORK OPERATIONS CENTER)

Evaluación de Riesgos: GENTE E INSTALACIONES

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Ausentismo del total de los Agentes de la Mesa de Servicios (enfermedad, incapacidad, accidente)	X						X	
Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)		X					X	
Incendio en las instalaciones.	X						X	
Sismo catastrófico.				X				X
Inundación catastrófica.		X					X	

Resultados de Estimación de Riesgo: GENTE E INSTALACIONES

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Ausentismo del total de los Agentes de la Mesa de Servicios (enfermedad, incapacidad, accidente, etc.)	1	3	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Incendio en las instalaciones.	1	3	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Sismo catastrófico.	4	4	I	Inaceptable	El riesgo debe ser reducido o si es posible eliminarlo inmediatamente. Situaciones donde los esfuerzos de recuperación son muy difíciles. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III o IV.
Inundación catastrófica.	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.

Evaluación de Riesgos: SISTEMAS DE TI, REDES Y PROCESOS

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Inoperatividad de las redes de voz y datos dentro del Site del NOC		X					X	
Daños en servidores de aplicación de monitoreo y administración		X						X
Falla en los equipos y consolas de monitoreo.			X				X	
Falla en el servicio de internet		X				X		
Falla en los enlaces de comunicaciones		X					X	

Resultados de Estimación de Riesgo: SISTEMAS DE TI, REDES Y PROCESOS

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Inoperatividad de las redes de voz y datos dentro del Site del NOC	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Daños en servidores de aplicación de monitoreo y administración	2	4	II	Indeseable	Implementación de planes de contingencia para evitar la interrupción de los servicios de la Mesa Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III.
Falla en los equipos y consolas de monitoreo.	3	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falla en el servicio de internet	2	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Evaluación de Riesgos: SERVICIOS CRÍTICOS (ENERGÍA, AGUA, TELÉFONO, ETC)

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Fallas de energía eléctrica.			X					X
Fallas del sistema telefónico.		X					X	
Falta de iluminación	X				X			
Falta de Agua	X				X			
Fallas en el sistema de enfriamiento		X					X	
Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)		X					X	

Resultados de Estimación de Riesgo: SERVICIOS CRÍTICOS (ENERGÍA, AGUA, TELÉFONO, ETC)

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Fallas de energía eléctrica.	3	4	I	Inaceptable	El riesgo debe ser reducido o si es posible eliminarlo inmediatamente. Situaciones donde los esfuerzos de recuperación son muy difíciles. Se deben tomar medidas de prevención y control para mitigarlo hasta un rango de riesgo III o IV.
Fallas del sistema telefónico.	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Falta de iluminación	1	1	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Falta de Agua	1	1	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Fallas en el sistema de enfriamiento	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.
Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)	2	3	III	Aceptable con controles	El riesgo se mitiga en gran parte con la implementación de controles que no requieren inversión en la implementación de planes de contingencia.

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

Evaluación de Riesgos: ACTIVOS CRÍTICOS (CONTRATOS, GARANTÍAS, ETC.)

EVENTOS CAUSANTES DEL RIESGO	PROBABILIDAD DE OCURRENCIA				SEVERIDAD DE LAS CONSECUENCIAS			
	1	2	3	4	1	2	3	4
Pérdidas de contratos y/o SLA's	X					X		
Pérdida de Procedimientos documentados	X					X		

Resultados de Estimación de Riesgo: ACTIVOS CRÍTICOS (CONTRATOS, GARANTÍAS, ETC.)

RESULTADOS DE MATRIZ DE RIESGOS	PROBABILIDAD DE OCURRENCIA	SEVERIDAD DE LAS CONSECUENCIAS	IMPORTANCIA	CATEGORÍA	ACCIONES QUE DEBEN TOMARSE
Pérdidas de contratos y/o SLA's	1	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.
Pérdida de Procedimientos documentados	1	2	IV	Aceptable como está	El riesgo es asumido tal y como está, no se toman medidas preventivas ni la implementación de planes de contingencia.

Resultado del análisis de riesgos

El análisis de riesgo efectuado nos arroja que los eventos con menos probabilidad de ocurrencia son:

- Ausentismo del total de los Agentes del NOC Especializado (enfermedad, incapacidad, accidente, etc.)
- Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)
- Incendio en las instalaciones.
- Inundación catastrófica.
- Inoperatividad de las redes de voz y datos dentro del Site del NOC
- Daños en servidores de aplicación de monitoreo y administración
- Falla en el servicio de internet
- Falta de iluminación
- Falta de agua
- Fallas en el sistema de enfriamiento
- Pérdidas de contratos y/o SLA's
- Pérdida de Procedimientos documentados

Por otra parte, los eventos que representarían mayor pérdida financiera tanto para el negocio del cliente como del NOC serían:

- Sismo catastrófico.
- Inoperatividad de las redes de voz y datos dentro del Site del NOC
- Falla en los equipos y consolas de monitoreo.
- Fallas de energía eléctrica.
- Falla en los enlaces de comunicaciones

Del mismo modo, existen eventos que requieren la implementación de controles para mitigar su impacto negativo como son:

- Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)
- Inundación catastrófica.
- Daños en servidores de aplicación de monitoreo y administración
- Fallas del sistema telefónico.
- Fallas en el sistema de enfriamiento
- Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)

El resultado arroja que son 10 eventos que requieren atender inmediatamente para evitar pérdidas que van de lo considerado a lo crítico en cuento al negocio, imagen del NOC, penalizaciones y daño a la infraestructura se refieren.

Las opciones de tratamiento más convenientes para cada evento se describirán en un documento anexo a este análisis de riesgos, donde se identificarán una gama de opciones de tratamiento de riesgos y su posterior implementación.

Las opciones de tratamiento que se enuncian a continuación no son limitativas ni serán apropiadas en todas las circunstancias.

EVITAR el riesgo. Se decide donde sea práctico, no proceder con servicios, procesos y/o actividades que podrían generar riesgos inaceptables, buscando con ello eludir el riesgo inherente asociado.

REDUCIR el riesgo. Se decide prevenir y/o reducir el riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al nivel más bajo posible, el cual debe ser compatible con las actividades del NOC. Se puede conseguir con la optimización de los procedimientos y la implementación de controles.

REDUCIR la probabilidad de ocurrencia. Prevención del riesgo a través de la implementación de acciones tendientes a controlar su frecuencia o probabilidad.

REDUCIR las consecuencias o **MITIGAR** el riesgo. Reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si este sucede.

ATOMIZAR el riesgo. El NOC puede segmentar "el objeto" sobre la cual recae la amenaza de riesgo o distribuir la localización de "los objetos".

TRANSFERIR el riesgo. El NOC puede decidir traspasar o trasladar riesgos a otra parte o lugar de manera total o parcial. Las trasferencias parciales son conocidas como COMPARTIR el riesgo. La localización o distribución del riesgo en diversos lugares se conoce como DISPERSIÓN o ATOMIZACIÓN del riesgo.

ASUMIR el riesgo. El NOC decide aceptar los riesgos como ellos existen en la actualidad y establece políticas y estrategias financieras apropiadas para su tratamiento. En este caso el NOC considera que el riesgo residual actual es de bajo nivel y decide convivir con él, aceptando la pérdida probable, con la cual las estrategias de prevención se vuelven esenciales.

Medidas de mitigación de riesgo

Las recomendaciones para poder manejar los diferentes riesgos que implica la operación de los servicios de Mesa de Servicios, Call Center Especializado y NOC se agrupan para poder ser tratados de acuerdo a su criticidad.

Las medidas que se enuncian a continuación no son limitativas:

RIESGO ALTO

RIESGO	ESTRATEGIA	ACCIONES
Sismo catastrófico.	REDUCIR, TRASLADO	Desarrollar plan de recuperación de desastres. Del resultado de dicho plan se valoría la implementación de un site secundario para recuperarse de una contingencia mayor. Contratación Póliza de Seguros para casos de desastres.
Inoperatividad de las redes de voz y datos dentro del Site del NOC	EVITAR	Implementar esquemas de alta disponibilidad. Desarrollar soluciones de clusters, políticas adecuadas de respaldo/recuperación.
Falla en los equipos y consolas de monitoreo.	REDUCIR	Implementar medidas de aumento en la disponibilidad. Sistemas centrales en cluster, servicios de mantenimientos preventivos, etc.
Fallas de energía eléctrica.	REDUCIR	Mantenimiento y mejoras del sistema de cableado y protección del sistema eléctrico. Revisiones periódicas de UPS, mantenimiento regular del generador eléctrico. Revisión y/o contratación de servicio de aprovisionamiento de combustible para planta generadora eléctrica.
Falla en los enlaces de comunicaciones	ATOMIZAR, TRALADAR	Para aquellos clientes que no puedan soportar la pérdida del servicio por más de 2 horas, proponer la implementación de un enlace redundante por ruta distinta a la principal.

RIESGO MEDIO-BAJO

RIESGO	ESTRATEGIA	ACCIONES
Bloqueo de los accesos a las instalaciones por eventos externos (bloqueos, manifestaciones, huelga, etc.)	REDUCIR	Implementación de soluciones de acceso a las aplicaciones de modo externo (portales de internet, control remoto, etc.)
Inundación catastrófica.	MITIGAR	Revisión periódica y/o reparación de los sistemas de desagüe. Instalación de bombas de desagüe.
Daños en servidores de aplicación de monitoreo y administración	REDUCIR	Implementar medidas de aumento en la disponibilidad. Sistemas centrales en cluster, servicios de mantenimientos preventivos, etc.
Fallas del sistema telefónico.	REDUCIR, ATOMIZAR	Desarrollar una estrategia de comunicación alterna, vía celulares, radios o inclusive mensajería instantánea.
Fallas en el sistema de enfriamiento	REDUCIR	Contratación de pólizas de mantenimiento. Redistribución en los sistemas de enfriamiento, esquemas de disponibilidad tipo N+1 para el caso de que falle alguno de los equipos.
Fallas en el sistema de control de acceso (evento de una acceso no autorizado en Site)	REDUCIR	Mejoras en los controles de acceso al site. Combinar controles biométricos y bitácoras de accesos. Instalación de cámaras de vigilancia.

SOA - DECLARATORIA DE APLICABILIDAD

(Medidas de mitigación de las amenazas y los riesgos)

Objetivo:

Adoptar los controles necesarios contenidos en el estándar internacional ISO/IEC 27001:2005, los cuales cubren todos los tipos de organizaciones (ejemplo. empresas comerciales, agencias de estatales, organizaciones no lucrativas, gubernamentales, etc.). Este estándar internacional especifica los requisitos para establecer, ejecutar, operar, supervisar, revisar, mantener y mejorar el documentó del Plan de Seguridad de CEPRA dentro del contexto de los riesgos totales del negocio de la organización.

Las listas en la tabla A.1 no son exhaustivas y una organización puede considerar que objetivos y controles adicionales son necesarios. Los objetivos y los controles de estas tablas serán seleccionados como parte del Plan de Seguridad de CEPRA.

Tabla A.1 Objetivos y Controles

A.5 Políticas de Seguridad		
A.5.1: Política de la seguridad de la información. Objetivo: Proporcionar la dirección y ayuda de la gerencia para la seguridad de la información de acuerdo con requisitos del negocio y leyes y regulaciones relevantes.		
A.5.1.1	Política de seguridad de la información	Emitido en el documento " Políticas de Seguridad de la Información"
A.5.1.2	Revisión de las políticas de seguridad de la Información	La última versión del documento emitido es la usada actualmente y no se han realizado aún modificaciones al mismo.
A.6 Seguridad de la Información en CEPRA		
A.6.1: Organización Interna Objetivo: Manejar la seguridad de la información dentro de CEPRA		
A.6.1.1	Administración de la seguridad de la información	La responsabilidad de la seguridad de la información dentro de CEPRA recae en las siguientes áreas y proveedor: • Dirección de Ingeniería • Gerencia de Infraestructura • NOC (CEPRA) • Especialistas ServiceCenter • Especialistas de Red • Netrix (Proveedor de SOC para CEPRA)
A.6.1.2	Coordinación de la seguridad de la información	La coordinación de la administración de las actividades de seguridad corresponde a: • Dirección de Ingeniería • Gerencia de Infraestructura

A.6.1.3	Rol de responsabilidades	Se tienen definido y actualizado un organigrama de CEPRA, además para cada puesto se dispone de una descriptiva del mismo en el cual se mencionan todas las responsabilidades	
A.6.1.4	Proceso de autorización para acceso a las instalaciones y tratamiento de información	Acceso a las instalaciones	Se definen los accesos en el documento "Políticas de Control de Acceso de CEPRA"
		Seguridad de acceso a la Información	Definida en el documento "Políticas de Seguridad de la Información"
A.6.1.5	Acuerdos de confidencialidad	El área de Recursos Humanos es quien se encarga de asegurarse de celebrar acuerdo de confidencialidad con los empleados de CEPRA	
A.6.1.6	Contacto con autoridades	Se dispone de un directorio con los teléfonos de las autoridades (organizaciones estatales y personal interno) correspondientes en caso de que se requiera su intervención durante alguna contingencia.	
A.6.1.7	Contacto con grupo de especialistas	Se tienen disponibles los medios para contactar al personal especialista con el que cuenta CEPRA en caso de presentarse alguna eventualidad.	
A.6.1.8	Revisores independientes de la seguridad de la información	NA	
A.6.2 Partes Externas Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso			
A.6.2.1	Identificación de riesgos relacionados con partes externas	Se han identificado algunos riesgos como son: control de acceso de datos para clientes, correo electrónico administrado por Mexis identificación y control de acceso a visitas	
A.6.2.2	Lineamientos de seguridad para con los clientes	Recepción y vigilancia	• Solicita identificación oficial y registra en bitácora a todo cliente, proveedor o personal sin identificación. • Personal de vigilancia permite acceso mediante su cuenta en el sistema biométrico
A.6.2.3	Lineamientos de seguridad en acuerdo con terceros	NA	
A.7 Administración de activos			
A.7.1 Responsabilidad por los activos Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales			
A.7.1.1	Inventario de Activos	Lo realiza el responsable de la CMDB de CEPRA mediante la herramienta ServiceCenter, esto se complementa con el monitoreo de hardware, software y dispositivos de red con la herramienta Altiris	
A.7.1.2	Propiedad de Activos	Esta información de correlación se mantiene en la CMDB mediante ServiceCenter	
A.7.1.3	Uso aceptable de los activos	Se especifica dentro del documento "Políticas de seguridad de la información "	
A.7.2 Clasificación de la Información Objetivo: Asegurar que la información reciba un apropiado nivel de protección			
A.7.2.1	Guías para clasificar la información	• Definido en el documento "Medidas preventivas BD Service Center" • En la administración de la DSL	

A.7.2.2	Etiquetado y resguardo de la información	• Definido en el documento "Medidas preventivas BD ServiceCenter" • En la administración de la DSL • Resguardo de respaldos de la BD ServiceCenter	
A 8. Seguridad de los Recursos Humanos			
A.8.1 Antes de contratación de empleados y proveedores. Objetivo: Asegurarse que los empleados, los contratistas y los usuarios de los terceros entiendan sus responsabilidades, para reducir el riesgo del hurto, fraude o el uso erróneo de los medios de información.			
A.8.1.2	Rol y responsabilidades	Las áreas de CEPRA con ayuda de recursos humanos	Establecen la descripción de puestos
A.8.1.3	Investigación	Recursos Humanos	Investiga y comprueba datos y perfiles de empleados
		Gerencia de Infraestructura	Valida datos y perfil de proveedores
A.8.1.4	Términos y condiciones de contratación	Recursos Humanos, Dirección de Operaciones, Dirección de Ingeniaría	Revisan y elaboran contrato de empleo, prestaciones y beneficios.
		Dirección de Ingeniería y Gerencia de Infraestructura	Tramita y modifica acuerdos mediante un contrato preestablecido para proveedores
A.8.2 Durante el contrato con el empleado o proveedor Objetivo: Asegurarse de que todos los empleados, los contratistas y los usuarios de terceros estén enterados de amenazas y preocupaciones de la seguridad de la información, sus responsabilidades, y estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal y reducir el riesgo del error humano.			
A.8.2.1	Administración de responsabilidades	• Se distribuye el documento "Política de Seguridad de la información" para CEPRA, así como se tienen indicaciones de uso en los lugares más críticos de CEPRA • En los contratos con proveedores se especifica la forma de conducirse dentro de las instalaciones de CEPRA • El acceso de visita y proveedores deberá ser siempre en compañía de personal de CEPRA, desde la entrada hasta la salida	
A.8.2.2	Conocimiento, educación y entrenamiento de la seguridad de la información	• Se distribuye el documento "Política de Seguridad de la información" para CEPRA, así como se tienen indicaciones de uso en los lugares más críticos de CEPRA • En los contratos con proveedores se especifica la forma de conducirse dentro de las instalaciones de CEPRA	
A.8.2.3	Proceso de disciplina	• Se distribuye el documento "Política de Seguridad de la información" para CEPRA, así como se tienen indicaciones de uso en los lugares más críticos de CEPRA	
A.8.3 Finalización de contratos con empleados y proveedores Objetivo: Asegurarse de que los empleados, los contratistas y los usuarios de terceros que salgan de la organización o cambien de empleo, lo hagan de una forma ordenada.			
A.8.3.1	Conclusión de responsabilidades	• Las condiciones se estipulan dentro del contrato para empleados • Las condiciones se estipulan dentro del contrato para proveedores.	
A.8.3.2	Retorno de activos	• Cada empleado o proveedor firma una responsiva por los	

		activos que le son asignados, la cual es devuelta al final del contrato y a la entrega y validación de buen estado de los mismos
A.8.3.3	Remoción de derechos de acceso	• Al final del contrato se eliminan cuentas de usuario en equipo de cómputo, correo electrónico, baja de registro de acceso en los equipos biométricos y se retiran tarjetas y credenciales de identificación.
A.9 Seguridad física y ambiental		
A.9.1 Áreas seguras Objetivo: Prevenir el acceso, daño e ingresos físicos desautorizados a las áreas seguras de la organización.		
A.9.1.1	Seguridad física de perímetro	• El acceso a las instalaciones de CEPRA está restringido por equipo de control de acceso biométrico • Todo empleado será identificado por su gafete credencial • El acceso por vía pública es video grabado día y noche • Toda actividad en áreas seguras es video grabada día y noche
A.9.1.2	Controles físicos de acceso	• El acceso a la áreas seguras está restringido por equipos biométricos. • Toda actividad en áreas seguras es video grabada día y noche
A.9.1.3	Seguridad de oficinas, cuartos e instalaciones	• El acceso a las instalaciones de CEPRA está restringido por equipo de control de acceso biométrico • Todo empleado será identificado por su gafete credencial • El acceso por vía pública es video grabado día y noche • Toda actividad en áreas seguras es videograbada día y noche
A.9.1.4	Protección contra elementos externos y ambientales	• Definidos en el documento Análisis de Riesgos
A.9.1.5	Trabajando en áreas seguras.	• El diseño de las instalaciones permite la rápida evacuación del inmueble • Se cuenta con extintores en caso de incendio en oficinas • Se cuenta con sistema contra incendió automático en el site de CEPRA.
A.9.1.6	Acceso público, entrega y áreas de carga	• Acceso a visitas y proveedores se encuentra restringido por una recepción y elementos de vigilancia así como por el sistema biométrico y de video vigilancia • El área de carga es independiente de la entrada principal y es vigilada con mediante cámaras de circuito cerrado.
A.9.2 Seguridad de los equipos Objetivo: Prevención, perdida, daño, o robo de activos o la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección de equipo	• El equipo principal de base de datos y ServiceCenter se encuentra ubicado en el Site de CEPRA • El acceso al Site de CEPRA es restringido por control de acceso biométrico • Toda actividad en áreas seguras es video grabada día y noche
A.9.2.2	Utilidades de soporte	• Todos los equipos de computo, red, telecomunicaciones, Servidores, sistemas de respaldo están soportados por un equipo UPS de 8 KVA regulados y una planta de emergencia

		de 125 KW
A.9.2.3	Seguridad de cableado	• El cableado eléctrico se encuentra debidamente protegido dentro de los ductos adecuados dentro del inmueble, con tableros de control resguardados en áreas aisladas. • El cableado de voz y datos se instalo bajo las mejores prácticas y certificaciones de desempeño y seguridad.

A.9.2.3	Mantenimiento de equipo	• Para el equipo de escritorio se cuenta con el área de remediación de CEPRA
		• Para los equipos servidores dentro del Site de CEPRA se tiene el respaldo de los fabricantes
		  • DELL
		• Se cuentan con contratos de mantenimiento para
		  • PBX
		  • UPS
		  • Planta de emergencia
		  • Clima

A.9.2.5	Seguridad para equipos fuera de las instalaciones	• Responsiva firmada por el usuario asignado • Antivirus • No existe acceso desde el exterior a la red de CEPRA • Acceso web solo a reportes y correo electrónico
A.9.2.6	Seguridad en la reutilización de equipo	• Los datos de un equipo a reutilizar son respaldados en otro disco duro, CD o DVD • El equipo a reutilizar deberá ser reconfigurado eliminando cualquier información y configuración previa, por el área de remediación
A.9.2.7	Extracción fuera de CEPRA	• Todo equipo es registrado a la salida de CEPRA • Todo el software se encuentra resguardado en la DSL
A.10 Comunicados y administración de la operación		
A.10.1 Procedimientos de operación y responsabilidades. Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.		
A.10.1.1	Documentación de procesos de operación	• Toda documentación o manual de proceso o procedimiento deberá encontrarse dentro de http://201.134.183.167:81/
A.10.1.1	Administración de cambios	• Los cambios a realizar en procesos, procedimientos y sistemas están controlados por el Sistema de Gestión de Calidad de los Servicios (ISO 20000) de CEPRA
A.10.1.2	Separación de Deberes	• Definidos en el documento descripción de puestos • Definidos en la matriz de roles y responsabilidades además de contar con un organigrama actualizado
A.10.1.3	Separación del desarrollo, pruebas y operaciones	• Las áreas de desarrollo, pruebas y operación se encuentran distribuidas entre la dirección de Ingeniería y la Dirección de Operaciones, con personal, roles y responsabilidades independientes.
A.10.2 Administración de la entrega de servicios por terceros Objetivo: Administrar la seguridad de la información y mantener acuerdos en la entrega del servicio de terceros.		
A.10.2.1	Servicios de Entrega	Se asegura la calidad del servicio mediante: • La firma de contratos • Recepción de SOW ó planes de trabajo.
A.10.2.2	Monitoreo y revisión de	• Mediante calendarios de mantenimiento

	servicios entregados por terceros	• Reportes de instalación, servicio y mantenimiento • Pruebas de desempeño. • Revisión y aprobación de entregables
A.10.2.3	Administración de cambios en los servicios de terceros	• Se realiza el requerimiento directo al proveedor vía telefónica, e-mail o sito Web • Se acuerdan y revisan modificaciones al contrato • Se modifican alcances originales en una nueva propuesta o actualización del SOW
A.10.3 Planeamiento y aceptación del sistema Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Administración de la capacidad	• Proceso descrito en el Sistema de Gestión de Calidad de los Servicios de CEPRA
A.10.3.2	Aceptación del sistema	• Cada especialista dueño de algún sistema se encarga de mantener actualizadas las versiones
A.10.4 Protección contra código malicioso Objetivo: Proteger la integridad del software y de la información		
A.10.4.1	Control contra código Malicioso	• Se ha implementado un software antivirus • Se mantiene activado el sistema de Firewall Juniper
A.10.4.2	Control contra códigos en sistemas móviles	• No se tienen liberadas conexiones para este tipo de dispositivos
A.10.5 Back-Up Objetivo: Mantener la integridad y disponibilidad de la información		
A.10.5.1	Respaldo de información	• Cada usuario de PC o laptop es responsable de su información • Para la base de datos de ServiceCenter se aplica el plan de contingencia ServiceCenter
A.10.6 Administración de la seguridad en la red Objetivo: Asegurar la protección de la información en la red y soporte a la infraestructura		
A.10.6.1	Control de la red	• La red de CEPRA se encuentra aislada física y lógicamente de cualquier otra de incluso de la de los clientes • Se tiene control sobre ancho de banda, puertos de acceso, aplicaciones, paquetes que fluyen sobre la red, mediante el equipo de Firewall Juniper
A.10.6.2	Seguridad en los servicios de red	• Para los servicios de seguridad de la red y acceso a internet se cuenta con los servicios del SOC de Netrix
A.10.7 Manejo de medios Objetivo: Para prevenir acceso no autorizados, modificación, retiro o destrucción de activos, e interrupción a actividades económicas.		
A.10.7.1	Administración de medios removibles	• Se aplica el procedimiento documentado de plan de medidas preventivas base de datos ServiceCenter • El resguardo de las cintas generadas está a cargo de personal autorizado
A.10.7.2	Eliminación de medios	• Los medios se eliminan conforme a los procedimientos documentados del área de soporte técnico
A.10.7.3	Procedimientos para el manejo de Información	• Cada usuario es responsable del manejo de su información en su PC o laptop • Los accesos a la base de datos de ServiceCenter es controlado por usuario y contraseña

		• Los respaldos de la base de datos son ejecutados por el NOC
A.10.7.4	Seguridad de la documentación de los sistemas	• Cada dueño de proceso o especialista a cargo de algún sistema es responsable del resguardo de la documentación correspondiente
A.10.8 Intercambio de Información Objetivo: Para mantener la seguridad en el intercambio de información y software dentro de la organización y cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas para el intercambio de la Información	• El intercambio de información dentro de CEPRA y entre clientes y proveedores se realiza vía e-mail administrado por Mexis • Se agregan leyendas de confidencialidad en la firma de los e-mail de salida
A.10.8.2	Acuerdos de intercambio	NA
A.10.8.3	Transito de medios físicos	NA
A.10.8.4	Mensajes electrónicos	• El intercambio de información dentro de CEPRA y entre clientes y proveedores se realiza vía e-mail administrado por Mexis • Se agregan leyendas de confidencialidad en la firma de los e-mail de salida • Mexis proporciona a CEPRA el servicio anti-spam y anti-virus para el trafico de e-mail
A.10.8.5	Sistema de información del negocio	• Se tiene un filtrado y control de tráfico mediante SonicWall sobre los enlaces de datos con los clientes
A.10.9 Sistema de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y el uso seguro de este.		
A.10.9.1	Comercio electrónico	NA
A.10.9.2	Transacciones en línea	NA
A.10.9.3	Información pública disponible	NA
A.10.10 Monitoreo Objetivo: Para detectar procesos no autorizados de información.		
A.10.10.1	Auditorias de logs	• Cada especialista a cargo de algún sistema de hardware, software o red se encarga de auditar los "logs" de sus sistemas o equipos
A.10.10.2	Monitorear uso del sistema	NA
A.10.10.3	Protección de la información de Logs	• Cada especialista a cargo de algún sistema de hardware, software o red se encarga de proteger o resguardar los "logs" de sus sistemas o equipos
A.10.10.4	Logs de los administradores y operadores	• Cada especialista a cargo de algún sistema de hardware, software o red se encarga de supervisar la actividad de los usuarios Administrador y operador en sus sistemas o equipos
A.10.10.5	Logs de fallas	• Cada especialista a cargo de algún sistema de hardware, software o red se encarga de dar seguimiento a los "logs" de falla
A.10.10.6	Sincronización de relojes	• Cada equipo PC, servidor o dispositivo de red sincroniza su reloj con el servidor ServiceCenter
A.11 Control de Acceso		
A.11.1 Requerimientos del negocio para el control de acceso Objetivo: Controlar el acceso a la información.		

A.11.1.1	Política de control de acceso	• Se establece en el documento "Políticas de control de acceso"
A.11.2 Administración de acceso a usuarios Objetivo: Asegurar el acceso autorizado de los usuarios y evitar accesos no autorizados a los sistemas.		
A.11.2.1	Registro de usuarios	• Se solicita registro de usuario para acceder a Service Center • Se solicita registro de usuario para el sistema de correo electrónico • Cada usuario maneja contraseña de acceso en sus equipos personales.
A.11.2.2	Privilegios de Administración	• El especialista de cada sistema es responsable del resguardo de las cuentas de administrador, operadores o súper usuarios de cada uno de sus sistemas.
A.11.2.3	Administración de contraseñas de usuario	• El especialista de cada sistema es responsable del resguardo de la administración de cuentas de usuarios y contraseñas para cada uno de sus sistemas o equipos.
A.11.2.4	Revisión de los derechos de acceso de usuarios	• El especialista de cada sistema es responsable de los derechos de acceso de cada usuario.
A.11.3 Responsabilidad de usuarios Objetivo: Prevenir accesos no autorizados y robo de información		
A.11.3.1	Uso de contraseña	• Cada usuario configura una contraseña de acceso a sus equipos personales
A.11.3.2	Equipo de usuario desatendido	• Cada usuario tendrá que configurar un protector de pantalla que se activará cierto tiempo después que el usuario se ausenta del equipo.
A.11.3.3	Política de escritorios y pantallas limpias	• Se le informa al usuario que debe de mantener su escritorio limpio, libre de papeles innecesarios así como de medios de almacenamiento removibles sin uso.
A.11.4 Control de Acceso a la Red Objetivo: Prevenir accesos no autorizados a la red.		
A.11.4.1	Políticas de uso de los servicio de Red	• Se establecen en el documento "Políticas de Seguridad de la Información"
A.11.4.2	Autenticación de usuarios para conexiones externas	NA
A.11.4.3	Identificación de equipos en la Red	• Los equipos se identifican por la dirección IP • Se instala el cliente de Altiris para el uso de Desktop Management
A.11.4.4	Diagnostico remoto y configuración de protección de puertos	• Se utiliza el Desktop Management • El sistema de Firewall Juniper controla el acceso desde Internet
A.11.4.5	Separación de Redes	• Las red de CEPRA se encuentra aislada lógica y físicamente de otras redes de clientes y compañías hermanas
A.11.4.6	Control de conexión de Red	• Las red de CEPRA se encuentra aislada lógica y físicamente de otras redes de clientes y compañías hermanas • No se tienen habilitados accesos desde internet
A.11.4.7	Control de Ruteo de Red	• El control de ruteo de red es controlado por el Firewall Juniper
A.11.5 Control de acceso al Sistema Operativo Objetivo: Prevenir accesos no autorizados al sistema operativo		
A.11.5.1	Procedimiento de firma segura	• Cada usuario configura una contraseña de acceso a sus equipos personales

		• Cada especialista configura las cuentas de acceso a los sistemas a su cargo
A.11.5.2	Identificación de usuario y autenticación	• Cada usuario configura una contraseña de acceso a sus equipos personales • Cada especialista designa una cuenta única de acceso por usuario.
A.11.5.3	Administración de contraseñas del sistema	• Cada usuario configura una contraseña de acceso a sus equipos personales y administra cuentas adicionales • Cada especialista configura y administra las cuentas de acceso a los sistemas a su cargo
A.11.5.4	Uso de utilerías de sistemas	• Son permitidos solo en ambiente de pruebas
A.11.5.5	Sesiones time-out	• El acceso a la base de datos de ServiceCenter desconecta usuarios inactivos.
A.11.5.6	Limitación del tiempo de conexión	NA
A.11.6 Control de acceso a información y aplicaciones Objetivo: Prevenir accesos no autorizados a información sostenida en aplicaciones.		
A.11.6.1	Restricción de acceso a Información	• Cada especialista con un sistema a su cargo crean usuarios de distinto nivel para cada uno de los servidores a su cargo
A.11.6.2	Aislamiento de sistemas Sensibles	NA
A.11.7 Sistemas móviles y teletrabajo Objetivo: Asegurar la seguridad de la información cuando se usen sistemas móviles o facilidades para el teletrabajo		
A.11.7.1	Computadoras móviles y comunicaciones	• El equipo de Wireless cuanta con seguridad activada
A.11.7.2	Teletrabajo	NA
A.12 Adquisición de sistemas, desarrollo y mantenimiento		
A.12.1 Requerimientos de seguridad para sistemas de información Objetivo: Asegurar que la seguridad es parte integral de los sistemas de información		
A.12.1.1	Requerimientos de seguridad, análisis y especificaciones	• Cada especialista a cargo de un sistema o equipo que requiere de modificaciones o nuevas adquisiciones determina los requerimientos de seguridad.
A.12.2 Proceso de correcciones a las aplicaciones Objetivo: Prevenir errores, perdidas, modificaciones no autorizadas indebidas de información en las aplicaciones.		
A.12.2.1	Validación de entrada de datos	• La validación de entrada de datos en ServiceCenter es aplicada por la propia interface de la aplicación y por los controles implícitos en SQL
A.12.2.2	Control interno de procesamiento	• La integridad de datos en ServiceCenter es aplicada por la propia interface de la aplicación y por los controles implícitos en SQL
A.12.2.3	Integridad de mensajes	• Se utiliza Outlook como cliente de correo electrónico para asegurar la creación, envío y recepción de mensajes de e-mail íntegros y seguros • Se dispone de un software antivirus instalado en cada equipo que asegura mensajes libres de virus
A.12.2.4	Validación de datos de Salida	NA
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad, e integridad de la información mediante métodos criptográficos		

A.12.3.1	Política de uso de controles criptográficos	NA
A.12.3.2	Manejo de llaves	NA
A.12.4 Seguridad del sistema de archivos Objetivo: Asegurar la seguridad del sistema de archivos.		
A.12.4.1	Control de software operacional	• La seguridad de los archivos está controlada por el sistema de archivos del propio sistema operativo.
A.12.4.2	Protección del sistema de prueba de datos	NA
A.12.4.3	Control de acceso a programas de código fuente	NA
A.12.5 Seguridad en el desarrollo y soporte de procesos Objetivo: Mantener la seguridad de aplicaciones, sistemas de software e información.		
A.12.5.1	Control de cambios de procedimientos	• El versionamiento de todos los documentos está controlado por la administración de cambios del Sistema de Gestión de Calidad de los Servicios de CEPRA
A.12.5.2	Revisión técnica de aplicaciones después de cambios en el sistema operativo	NA
A.12.5.3	Restricciones sobre cambios en paquetes de software	NA
A.12.5.4	Extracción de información	NA
A.12.5.5	Desarrollo de software por terceros	NA
A.12.6 Técnicas del manejo de vulnerabilidad Objetivo: Reducir el riesgo resultado de la publicación de técnicas de vulnerabilidad.		
A.12.6.1	Control de técnicas de vulnerabilidad	• Estos controles se establecen en el firewall Juniper de acceso a Internet
A.13 Administración de incidentes de la seguridad de la información		
A.13.1 Reportes de eventos y debilidades de la seguridad de la información Objetivo: Asegurar que los eventos y debilidades relacionados con la seguridad de la información son comunicados de manera que se tomen medidas correctivas a tiempo.		
A.13.1.1	Reporte de eventos en la seguridad de la información	• La herramienta ServiceCenter permite categorizar los incidentes que son levantados en la mesa de servicios relacionados con la seguridad de la información
A.13.1.2	Reporte de debilidades en la seguridad	NA
A.13.2 Administración de incidentes y mejoras de la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	• Se tienen determinados mediante una matriz los roles y responsabilidades para la administración de la seguridad de la información
A.13.2.2	Aprendizaje a partir de los incidentes de seguridad de la información	• La herramienta ServiceCenter, permite registrar el aprendizaje de los incidentes de seguridad
A.13.2.3	Colección de evidencia	NA
A.14 Administración de la continuidad del negocio		
A.14.1 Administración de la continuidad del negocio en aspectos de la seguridad de la información.		

Objetivo: Para contrarrestar interrupciones a las actividades económicas y proteger procesos críticos del negocio contra efectos de caídas importantes de los sistemas ante desastres en la información y asegurar su restauración oportuna.		
A.14.1.1	Incluir la seguridad en el plan de continuidad del negocio	• CEPRA dispone de procedimientos y políticas documentadas para la administración de la continuidad y disponibilidad del negocio; así mismo dispone de planes de contingencia y formatos registrar y evidencia las pruebas realizadas al plan de continuidad del negocio.
A.14.1.2	Continuidad del negocio y elementos de riesgo	
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo la seguridad de la información	
A.14.1.4	Marco del plan de continuidad del negocio	
A.14.1.5	Pruebas y mantenimiento del plan de continuidad del negocio	
A.15 Conformidades		
A.15.1 Conformidades con requerimientos Legales Objetivo: Evitar violaciones de cualquier ley, obligación regulatoria o contractual y de cualquier requerimiento de seguridad.		
A.15.1.1	Identificar la aplicabilidad de la legislación	• El departamento jurídico de CEPRA es quien se encarga de asegurarse de que se cumplan las leyes, obligaciones regulatorias y contractuales en materia de seguridad.
A.15.1.2	Derechos de propiedad intelectual	
A.15.1.3	Protección de los registros de CEPRA	
A.15.1.4	Protección y privacidad de información personal	
A.15.1.5	Prevención del uso inadecuado de información	
A.15.1.6	Regulación de controles criptográficos	
A.15.2 Conformidad con políticas de seguridad, estándares y técnicas de compatibilidad Objetivo: Asegurar la compatibilidad de sistemas con políticas de seguridad organizacional y estándares.		
A.15.2.1	Conformidad con políticas de seguridad y estándares	• Cada uno de los controles deberá apegarse a lo establecido en el Sistema de Gestión de Calidad de los Servicios de CEPRA
A.15.2.2	Técnicas de verificación de compatibilidad	
A.15.3 Consideraciones de auditoría de los sistemas de información Objetivo: Maximizar la efectividad y minimizar la interferencia del proceso de auditoría de los sistemas de información.		
A.15.3.1	Controles de auditoría de los sistemas de información	• Cada especialista dueño de un sistema o equipo aplica las políticas de auditoría convenientes
A.15.3.2	Protección de la información mediante herramientas de auditoría	• Cada especialista dueño de un sistema o equipo aplica las políticas de auditoría convenientes

METODOLOGÍA PARA ELABORACIÓN DEL PLAN DE CONTINUIDAD Y DISPONIBILIDAD

Objetivo

Proporcionar los mecanismos que garanticen la continuidad del negocio ante la ocurrencia de un evento súbito que provoque la interrupción de las operaciones de CEPRA.

Alcance

Este procedimiento aplica a todos los proyectos vigentes que involucren soluciones y/o servicios de CEPRA que se encuentren en su ciclo de vida dentro de los procesos de implementación de la solución y/o prestación del servicio.

Definiciones, Abreviaciones y Símbolos

1. **Activos:** Recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

2. **Amenazas**: Cosas que les pueden pasar a los activos causando un perjuicio a la Organización.

3. **Controles:** Son elementos de defensa desplegados para que aquellas amenazas no causen [tanto] daño. Con estos elementos se puede estimar:
   - **Impacto:** lo que podría pasar
   - **Riesgo:** lo que probablemente pase

4. **Modelo de valor:** Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

5. **Mapa de riesgos:** Relación de las amenazas a que están expuestos los activos.

6. **Evaluación de Controles:** Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

7. **Estado de riesgo:** Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

8. **Informe de insuficiencias:** Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

9. **Plan de seguridad:** Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos

10. **Seguridad**: Es la continuidad de las redes, los sistemas de información y de la infraestructura de soporte para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

11. **Disponibilidad:** Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

12. **Integridad:** Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización.

13. **Confidencialidad:** Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad pueden darse fugas y filtraciones de información, así como accesos no autorizados.

14. **Autenticidad (de quién hace uso de los datos o servicios):** Que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores. Contra la autenticidad se dan suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la base para poder luchar contra el repudio y, como tal, fundamenta el comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.
    Todas estas características pueden ser requeridas o no dependiendo de cada caso.
    Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición.

15. **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
    El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

16. **Análisis de riesgos:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

17. **Gestión de riesgos:** Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.
    Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio.

    Como todo esto es delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

Documentos Relacionados

1. Procedimiento de Ventas
2. Acciones Correctivas y Preventivas
3. Procedimiento para el Control de Documentos
4. Procedimiento para el Control de Registros
5. Procedimiento de Administración de Cambios
6. Procedimiento de Administración de Niveles de Servicio
7. Diagrama de Flujo de la Administración de la Disponibilidad y Continuidad
8. Diagrama de Flujo de la Administración de la Disponibilidad y Continuidad

Política(s)

El Administrador de Continuidad:

- Deberá apegarse y cumplir con este procedimiento.
- Asegurar que los acuerdos de continuidad y disponibilidad comprometidos con los clientes sean cumplidos en todas las circunstancias.
- Identificar los requisitos de continuidad y disponibilidad del servicio con base a los planes del negocio, SLA´s y análisis de riesgos.
- Incluir los lineamientos, accesos, tiempos de reacción, recuperación y disponibilidad final de los componentes del sistema dentro del Plan de Disponibilidad y Continuidad.
- Desarrollar los planes de Disponibilidad y Continuidad y revisarlos anualmente, en caso de que no sufran cambios o modificaciones, de ser así se revisaran en cada actualización o cambio.
- Mantener el Plan de Disponibilidad y Continuidad actualizado, para asegurar que se reflejan los cambios convenidos y requeridos por el negocio.
- El proceso de administración de Cambios debe valorar el impacto de cualquier cambio en el Plan de Disponibilidad y Continuidad del servicio.
- Medir y registrar la disponibilidad en los Reportes de Niveles de Servicio.
- Investigar la no disponibilidad y realizar acciones correctivas y preventivas para que esta no vuelva a ocurrir.
- Incluir dentro del Plan de Disponibilidad y Continuidad listas de contactos y CMDB´s de los servicios proporcionados.
- Incluir dentro del Plan de Disponibilidad y Continuidad los accesos alternos cuando el acceso normal a las instalaciones sea impedido.
- Realizar el Plan de Disponibilidad y Continuidad de acuerdo a las necesidades del negocio.
- Realizar pruebas de Disponibilidad y Continuidad y registrar éstas, de no realizarse serán manejadas con Acciones Correctivas y preventivas
- Es responsabilidad del Administrador de la Disponibilidad y Continuidad, el resguardo de la información generada en este procedimiento conforme lo establece el Procedimiento para Control de Registros

Procedimiento y Responsabilidad

Administrador de Disponibilidad y Continuidad / Responsable de Desarrollo de Nuevas Soluciones y Servicios

1.1 Realizan análisis de los requerimientos de Disponibilidad y Continuidad de cada servicio.

1.2 Realizan el Análisis de Riesgos conforme a la Ficha Técnica para la Elaboración del Análisis de Riesgo enfocado a la disponibilidad y continuidad.

1.3 Identifican los eventos a atender derivados del Análisis de Riesgos.

1.4 Identifican los controles de Disponibilidad y Continuidad necesarios para atender los eventos detectados.

1.5 Elaboran el Plan de Disponibilidad y el Plan de Continuidad

1.6 Envían al Coordinador del SGCS el Plan de Disponibilidad y Continuidad

Coordinador del Sistema de Gestión de Calidad de los Servicios

1.7 Recibe el Plan de Disponibilidad y Plan de Continuidad y convoca reunión con el Comité de Calidad de CEPRA.

Comité de Calidad de CEPRA

1.8 Recibe y revisa el Plan de Disponibilidad y Plan de Continuidad

Si el Comité de Calidad está de acuerdo con el Plan de Disponibilidad y Plan de Continuidad realiza la actividad 1.12 en caso contrario realiza la actividad 1.9

1.9 Realiza sus observaciones al Plan de Disponibilidad y Plan de Continuidad y devuelve para su corrección al Coordinador del Sistema de Gestión de Calidad de los Servicios

Coordinador del Sistema de Gestión de Calidad de los Servicios

1.10 Recibe el Plan de Disponibilidad y Plan de Continuidad

1.11 Regresa el Plan de Disponibilidad y Plan de Continuidad al Responsable de Desarrollo de Nuevos Servicios Soluciones y Servicios y/o Administrador de Disponibilidad y Continuidad para su corrección y regresa a la actividad número 1.5.

Comité de Calidad de CEPRA

1.12 Autoriza el Plan de Disponibilidad y Plan de Continuidad y lo devuelve al Coordinador del Sistema de Gestión de Calidad de los Servicios

Coordinador del Sistema de Gestión de Calidad de los Servicios

1.13 Recibe el Plan de Disponibilidad y Plan de Continuidad autorizados y los envía al Administrador de Disponibilidad y Continuidad.

Administrador de Disponibilidad y Continuidad

1.14 Recibe el Plan de Disponibilidad y Plan de Continuidad autorizados.
1.15 Implementa el Plan de Disponibilidad y Plan de Continuidad

Continúa con el Diagrama de Flujo de Administración de Disponibilidad y Continuidad

Administrador de la Disponibilidad y Continuidad

1.1 Recibe por parte del Administrador de Niveles de Servicio los requerimientos de la disponibilidad y continuidad del cliente en el Cuestionario Inicial de Requerimientos

11. Recibe por parte del Responsable de Desarrollo de Nuevas Soluciones y Servicios requisición de modificaciones o creación de un nuevo servicio.

1.2 Realiza análisis de los requerimientos de disponibilidad y continuidad del cliente en conjunto con el Administrador de Niveles de Servicio.

1.3 Elabora la solución referente a la disponibilidad y continuidad y lo envía al Administrador de Niveles de Servicio y éste lo entrega al área de Ventas.

Continúa con el Procedimiento de Ventas

1.4 Solicita al Administrador de Niveles de Servicio copia del contrato y/o SLA firmado para asegurar el cumplimiento de los estándares de disponibilidad y continuidad acordados.

Si el SLA está integrado al contrato continúa con la actividad número 1.5, en caso contrario continúa con la Etiqueta de ELABORACIÓN DE LA SECCIÓN DE CONTINUIDAD Y DISPONIBILIDAD EN EL SLA.

1.5 Recibe copia del contrato y/o SLA firmado por el cliente y revisa los estándares de disponibilidad y continuidad acordados.

1.6 Revisa el Análisis de Riesgos enfocado a la disponibilidad y continuidad.

Si existen nuevos eventos a atender, continúa con la actividad número 1.7, en caso contrario, continúa con la actividad número 1.11.

1.7 Identifica los eventos a atender derivado del Análisis de Riesgos.

1.8 Actualiza el Análisis de Riesgos enfocado a la Disponibilidad y Continuidad.

1.9 Elabora RFC y envía al Administrador de Cambios.

Continúa con el procedimiento de Administración de Cambios

1.10 Recibe notificación de la implementación del cambio por parte del Administrador de Cambios vía e-mail.

1.11 Implementa el Plan de Disponibilidad y Continuidad.

1.12 Elabora los reportes de niveles de servicio acordados en el SLA y/o Contrato.

1.13 Envía los reportes de los niveles de servicio referentes a la disponibilidad y continuidad al Administrador de Niveles de Servicio, Administrador de Problemas, Administrador de Incidentes, Administrador de Capacidad y a los interesados en esta información.

Si no existen incumplimientos, se da fin al proceso, en caso contrario se realiza el Procedimiento para Acciones Correctivas y Preventivas y regresa a la actividad número 1.12.

Etiqueta de Elaboración de la Sección de Disponibilidad y Continuidad en el SLA

1.1 Elabora la sección de SLA referente a la Disponibilidad y Continuidad en coordinación con los especialistas involucrados tomando como referencia la propuesta técnica y económica.

1.2 Envía la sección de disponibilidad y continuidad del SLA al Administrador de Niveles de Servicio.

Administrador de Niveles de Servicio

1.3 Recibe la sección de Disponibilidad y Continuidad del SLA y revisa.

Si no está de acuerdo realiza la actividad 1.4 en caso contrario continua con el procedimiento de Administración de Niveles de Servicio

1.4 Realiza sus observaciones y devuelve para su corrección y continúa con la actividad 1.1.

Regresa a Etiqueta de elaboración de la Sección de Seguridad en el SLA.

DRP - Plan de Recuperación de Desastres

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

PLAN DE RECUPERACIÓN DE DESASTRES

Introducción

Un desastre se define como cualquier evento accidental, natural o malicioso que amenaza o interrumpe las operaciones o servicios normales, causando con ello la "no disponibilidad" de los servicios informáticos por un tiempo tal que, para restablecer estos servicios, es necesario utilizar facilidades alternas de cómputo y telecomunicaciones en un sitio alterno.

Para poder restablecer estos servicios se hace necesario planear, desarrollar, probar y llevar a cabo procedimientos y planes que aseguren la óptima recuperación de estos servicios, documentando las estrategias, personal, procedimientos y recursos que serán utilizados para responder ante interrupciones que afecten la infraestructura de TI.

El plan de recuperación de TI es responsabilidad primaria de la Dirección General de la empresa; sin embargo, es la Dirección de Infraestructura la que tiene la responsabilidad de su desarrollo, mantenimiento y ejecución.

La necesidad de considerar un plan para recuperar los servicios de TI se desprende tanto de la posibilidad de un incidente que interrumpa la operación normal de CEPRA por un corto período, como de eventos catastróficos que impidan la continuidad del negocio.

Este plan ha sido diseñado para crear una serie de actividades que permitan a CEPRA dar respuesta inmediata y desempeñar actividades de recuperación luego del reconocimiento de cualquier interrupción no planeada de los servicios de TI que afecten la continuidad de las operaciones. Anexo a este plan se encuentran los planes de contingencia que deben ser puestos en marcha para la recuperación de los servicios de TI que CEPRA ofrece.

Objetivo

Este Plan de Recuperación de Desastres fue desarrollado para alcanzar los siguientes objetivos específicos:

1. Dar continuidad a los servicios informáticos de CEPRA en caso de presentarse una situación de contingencia mayor o catastrófica.
2. Proveer un enfoque organizado para el manejo de las actividades de respuesta y recuperación luego de un incidente no planeado o de una interrupción prolongada de los servicios.
3. Ofrecer respuestas oportunas y apropiadas a cualquier incidente no planeado, reduciendo así el efecto negativo de una interrupción de los servicios de cómputo.
4. Recuperar las aplicaciones críticas del negocio de manera oportuna, incrementando la habilidad de la compañía para recuperarse de una pérdida o daños a las instalaciones y servicios.

Estrategia de Recuperación

El presente plan se ejecutará cuando se haya presentado un evento que interrumpa las actividades del área de Tecnología, primordialmente y antes de cualquier acción se procederá a verificar la disponibilidad, el estado de los recursos humanos, materiales y tecnológicos del área, para reiniciar con la reinstalación de los sistemas. Ver anexos de este documento.

Invocación

Ante una situación de desastre, las únicas personas que pueden declarar la activación de este plan general de recuperación son:

- Director General de CEPRA
- Director de Infraestructura

Lineamientos Generales

- El carácter de este DRP es confidencial y la activación del mismo sólo puede ser determinada por los cargos descritos en el apartado "Invocación".
- El presente plan deberá ser revisado y adecuado a las necesidades y características del negocio cada 6 meses.
- Las pruebas a la efectividad del plan de recuperación se deben realizar en su totalidad al menos una vez al año. Durante las pruebas se deberá verificar la funcionalidad de los planes de contingencia del plan, la respuesta a la emergencia
- Este documento deberá ser resguardado en electrónico y en físico en algún sitio alterno que disponga la Dirección General, así mismo, la ubicación que se determine deberá ser del conocimiento del equipo de recuperación.
- El área de Infraestructura será la responsable de la custodia de este documento y de los demás documentos relacionados a este plan.

Dependencias

En adición a la activación de este plan, es necesario que para asegurar que el plan de recuperación será efectivamente aplicado se disponga de los siguientes documentos:

- Plan de contingencia red de datos
- Plan de contingencia ServiceCenter
- Plan de contingencia telefonía
- Plan de contingencia energía eléctrica

Equipo de Recuperación

Puesto	Detalles de Contacto	Suplentes	Detalles de Contacto
Director de Infraestructura		Gerente de Infraestructura	
Gerente de Infraestructura		Ingenieros de Soporte	
Director de Finanzas		Gerente de Finanzas	

Lista de Verificación del Equipo de Recuperación

A continuación se mencionan las actividades generales que el Equipo de Recuperación debe considerar al poner este plan en práctica.

ACTIVIDADES	CUMPLIMIENTO ACTUAL	OBJETIVO DE CUMPLIMIENTO
Confirmar la activación del Plan de Recuperación de Desastres		
Comenzar con las llamadas para la integración del equipo de recuperación		
Identificar situaciones y avisar al equipo de gestión de crisis		
Organizar los respaldos y registros vitales a ser enviados desde el sitio de almacenaje hasta el sitio de recuperación		
Establecer equipo de recuperación		
Confirmar el progreso de los requisitos de reporteo		
Informar al equipo de recuperación los requisitos para presentación de informes		
Confirmar las necesidades de enlace con otros equipos de recuperación		
Iniciar acciones de recuperación		
Notificar la estimación de recuperación de los sistemas y comienzo de las pruebas		
Notificar la estimación de cuando estarán listos los sistemas para el procesamiento de los usuarios.		

ANEXOS DEL DRP

- **F-1 Plan de contingencia red de datos**
- **F-2 Plan de contingencia ServiceCenter**
- **F-3 Plan de contingencia energía eléctrica**
- **F-4 Plan de contingencia telefonía**
- **F-5 Políticas generales de seguridad de CEPRA**

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

F-1 PLAN DE CONTINGENCIA RED DATOS

Objetivo:

Describir el procedimiento para recuperar las actividades críticas de operación, en caso de interrupciones parciales o totales por causa de fallas en los equipos activos de la Red Local de Datos, para mantener los servicios de operación al 99.9%.

Alcance:

- Mesa de Servicios
- Call Center
- NOC

Condiciones para la ejecución del Plan:

Responsabilidad: Este plan deberá ser ejecutado por o bajo la supervisión de los elementos de la Gerencia de Infraestructura

Cuando se ejecuta: Se ejecuta cuando se detecta una falla de conexión entre las estaciones de trabajo de la Mesa de Servicios, Call Center y/o NOC, con la Base de datos del Servidor "ServiceCenter"

Autorización: No hay pre-autorización para la ejecución, no hay firma de autorización

Notificaciones: Se notifica a la Gerencia de Infraestructura

Prioridad de Llamada	Tel. 53402700 Ext.	Nombre	Celular	e-mail
1	**a) Telefono, Nombre, celular, e-mail se eliminan** **FUNDAMENTO LEGAL:** Artículo 3 fracción II, 18 fracciones I y II, y 19 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el segundo párrafo del Segundo Transitorio y primer párrafo del Cuarto Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública publicada en el Diario oficial de la Federación el 09 de mayo de 2016, así como en el Lineamiento Trigésimo Octavo, Trigésimo noveno y Cuadragésimo, de los Lineamientos Generales para la Clasificación y Desclasificación de la información de las dependencias y entidades de la Administración Pública Federal publicado en el mismo órgano de difusión el 15 de abril de 2016. **Motivación:** Datos personales y/o datos financieros y/o patrimonial			
2				
3				

Pre-conocimiento: Los elementos que ejecuten este plan deberán contar con conocimientos acerca de:

- Conceptos de redes LAN
- Conceptos de cableado
- Ubicación de los equipos activos de Red en el Site de CEPRA

Material y datos requeridos antes de inicio:

- Memoria técnica de la arquitectura de Red LAN
- Lista de direcciones asignadas para los equipos de la Mesa de Servicios, Call Center, NOC, y ServiceCenter.

Precauciones: Considerar las condiciones de acceso a los siguientes sistemas:
Acceso restringido al Site de Comunicaciones (deberá tener autorización en el sistema de control de acceso de CEPRA).

Procedimiento:

- Monitoreo del comportamiento:

Se realiza diariamente la comprobación de disponibilidad de acceso sobre a Red Local hacia el Servidor de Service Center

- Declaración de Emergencia:

Se declara una emergencia en el momento que se pierden todas las conexiones de Red desde las estaciones de trabajo de la Mesa de Servicios, Call Center y NOC hacia el servidor de ServiceCenter.

Procedimiento de Reanudación

- Tiempo de Reanudación: 15 minutos
- Acciones: Se sustituye el Switch de conexión de red por un equipo de la misma cantidad de puertos de conexión, velocidad y características de operación, almacenado en CEPRA
- Equipos y/o Servicios Críticos en el Tiempo: Conexión de Red Local hacia el Servidor ServiceCenter

Procedimiento de Recuperación

- Tiempo de recuperación: 0
- Acciones: Se mantiene la operación establecida en el proceso de reanudación
- Equipo y/o Servicios Complementarios: Ninguno

Procedimiento de Restauración

- Tiempo de restauración: 0
- Acciones: Se puede determinar operación normal con la sustitución del equipo
- Recomendaciones: Prever contar con un equipo de respaldo en óptimas condiciones para utilizarlo en caso de contingencia, así como contar con la información de ubicaciones de equipos, estaciones de trabajo y servidores

- Conclusiones: Con base al Plan de Contingencia y recomendaciones de la Red Local de CEPRA antes descrito se puede concluir que el servicio de atención al cliente está cubierto en un 99.999 %

Matriz de Pruebas Post-Contingencia:

Establecer las pruebas a realizar una vez superada la contingencia para asegurar que la operación es normal

No	Prueba	Resultado esperado	Firma y Fecha de aceptado
1	Probar conectividad entre equipos	Conexión satisfactoria entre equipos	
2	Probar accesos a servicios de red	Conexión satisfactoria a los servicios de red por parte de los equipos	

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

F-2 PLAN DE CONTINGENCIA SERVICECENTER

Objetivo:

Describir el procedimiento para recuperar las actividades críticas de operación, en caso de interrupciones parciales o totales por causa de fallas en el ServiceCenter, para mantener los servicios de operación al 99.9% en los horarios de servicios de los clientes soportados en la herramienta.

Alcance:

- Mesa de Servicios

Condiciones para la ejecución del Plan:

Responsabilidad: Este plan deberá ser ejecutado por o bajo la supervisión de los elementos de la Mesa de Servicios y para recuperación de datos por el especialista en ServiceCenter.

Cuando se ejecuta: Se ejecuta cuando se detecta una interrupción total de la herramienta ServiceCenter.

Autorización: No hay pre-autorización para la ejecución.

Notificaciones: Se notifica a la gerencia de operaciones.

Prioridad de Llamada	Tel. 53402700	Nombre	Celular	e-mail
1	a) Teléfono, Nombre, celular, e-mail se eliminan **FUNDAMENTO LEGAL:** Artículo 3 fracción II, 18 fracciones I y II, y 19 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el segundo párrafo del Segundo Transitorio y primer párrafo del Cuarto Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública publicada en el Diario oficial de la Federación el 09 de mayo de 2016, así como en el Lineamiento Trigésimo Octavo, Trigésimo noveno y Cuadragésimo, de los Lineamientos Generales para la Clasificación y Desclasificación de la información de las dependencias y entidades de la Administración Pública Federal publicado en el mismo órgano de difusión el 15 de abril de 2016. **Motivación:** Datos personales y/o datos financieros y/o patrimonial			
2				

Pre-conocimiento: Los elementos que ejecuten este plan deberán contar con conocimientos acerca de:

- ServiceCenter
- Contraseña de acceso al sistema ServiceCenter

Material y datos requeridos antes de inicio:

- ServiceCenter
- Contraseña de acceso al sistema ServiceCenter
- Plan de Contingencia ServiceCenter

Precauciones. Considerar las condiciones de acceso a los siguientes sistemas:

- Contar con claves de acceso de administrador al ServiceCenter.

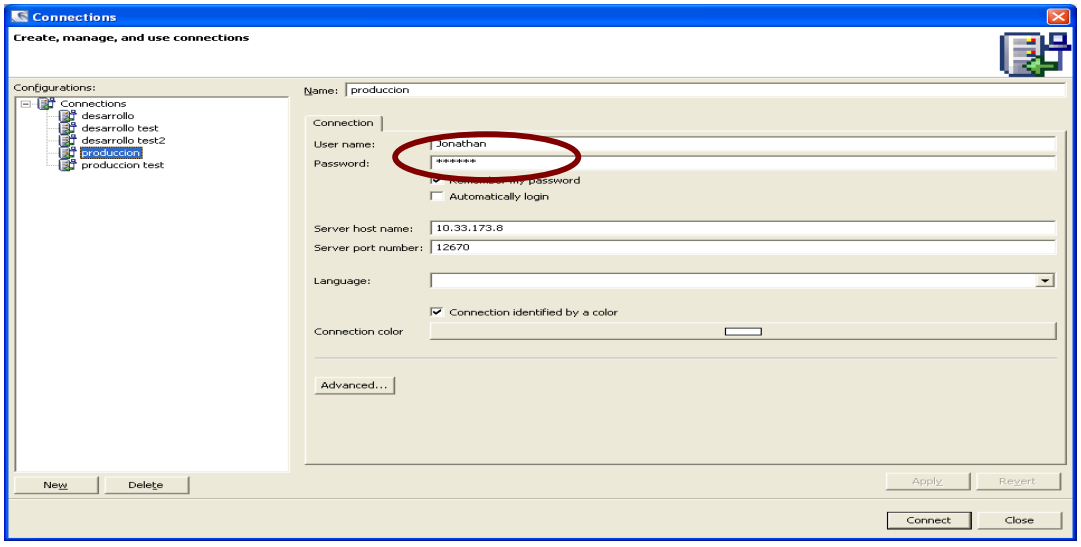
Procedimiento de Reanudación:

Tiempo de Reanudación: 3 minutos

Acciones:

1. Procedimiento de emergencia Cambio de servidor productivo a respaldo de producción.

1.1 Cuando quede abajo el servidor productivo los operadores de la Mesa de Servicios tendrán que entrar a la parte de conexión de su ServiceCenter y en esa parte tendrán que ajustar la IP de su Conexión al servidor de Respaldo.



1.2 Dentro del Parámetro Server Host Name poner la dirección 10.33.173.15

1.3 El usuario y la contraseña serán los mismos que en la instancia de producción.

1.4 Todas las pantallas y los privilegios serán los mismos que el ambiente de producción. La diferencia es que les dará los números diferentes al consecutivo del que les da comúnmente.

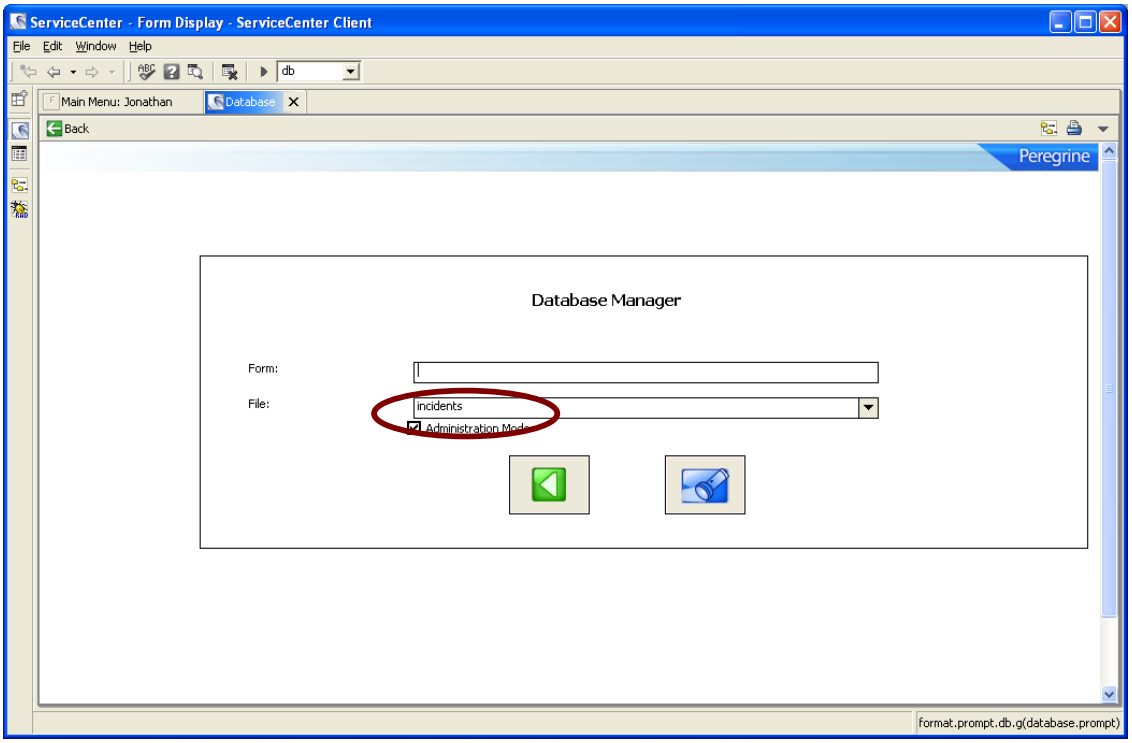
Procedimiento de Recuperación

Tiempo de recuperación: 10 minutos

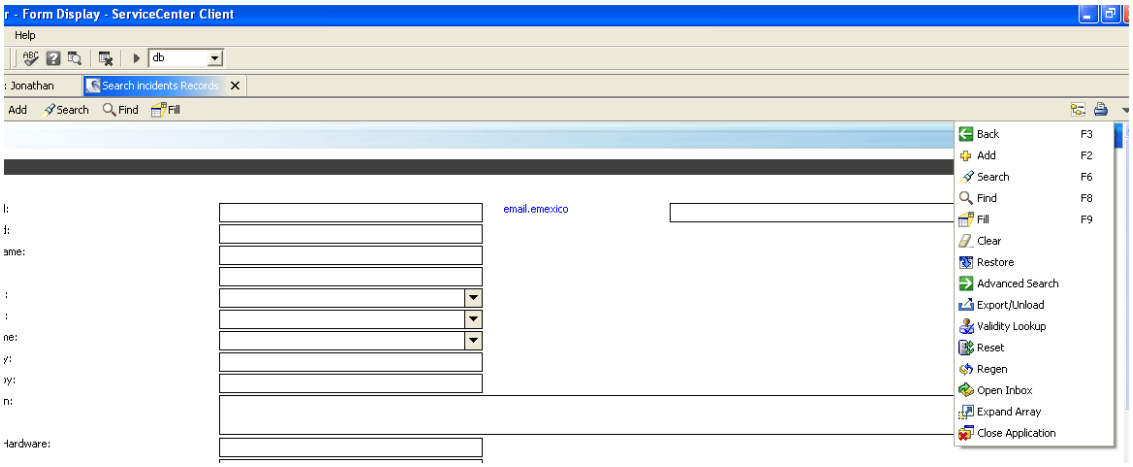
Acciones:

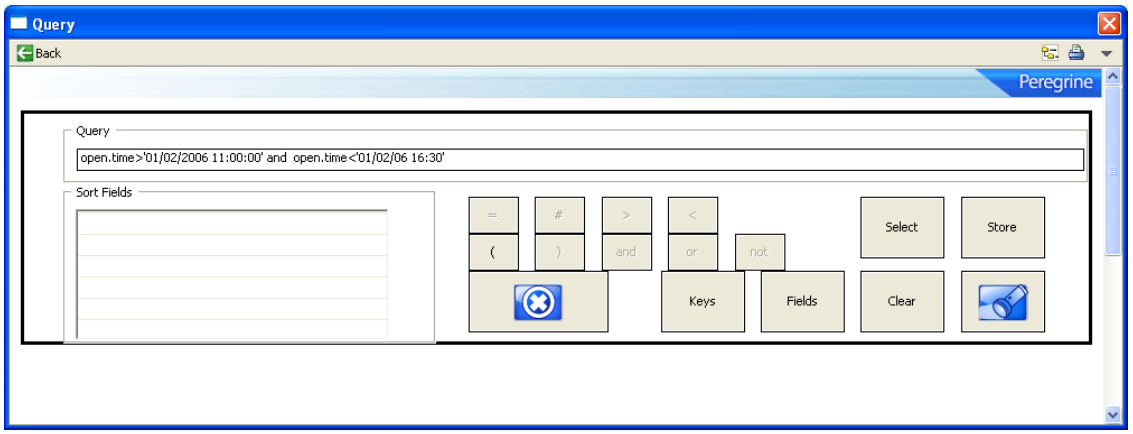
1.1 Para pasarlos a producción una vez restaurado el servicio será con las opciones de exportar del ServiceCenter se descargaran llamadas, incidentes y en caso de que los catálogos de activos o direcciones fueran modificados se cargaran los cambios.

1.2 El bajar la información del ambiente de respaldo será por medio del modulo de DB de ServiceCenter buscando el *file* que se requiere bajar.

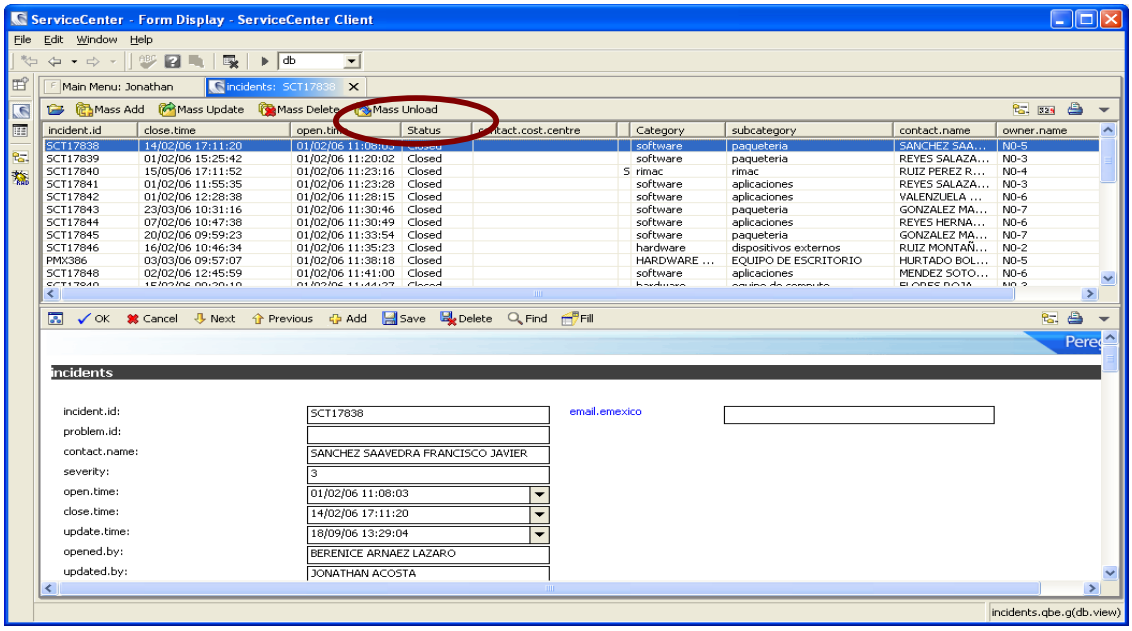


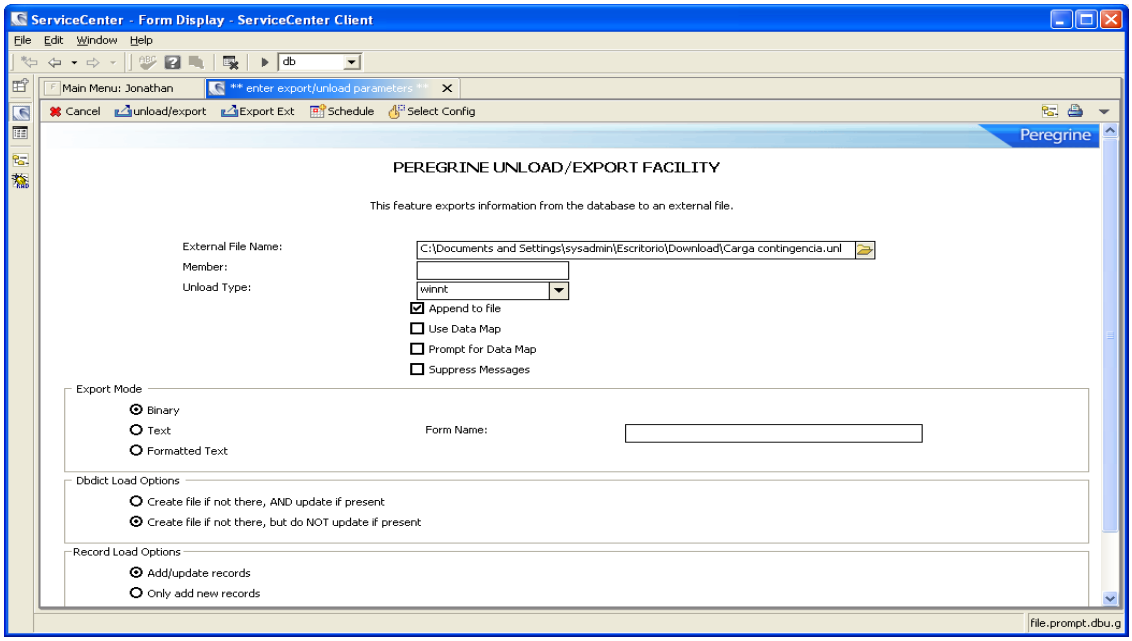
1.3 Para la búsqueda se realizara una búsqueda avanzada para buscar por fechas de apertura los incidentes y llamadas y por fechas de modificación los cambios a los catálogos.





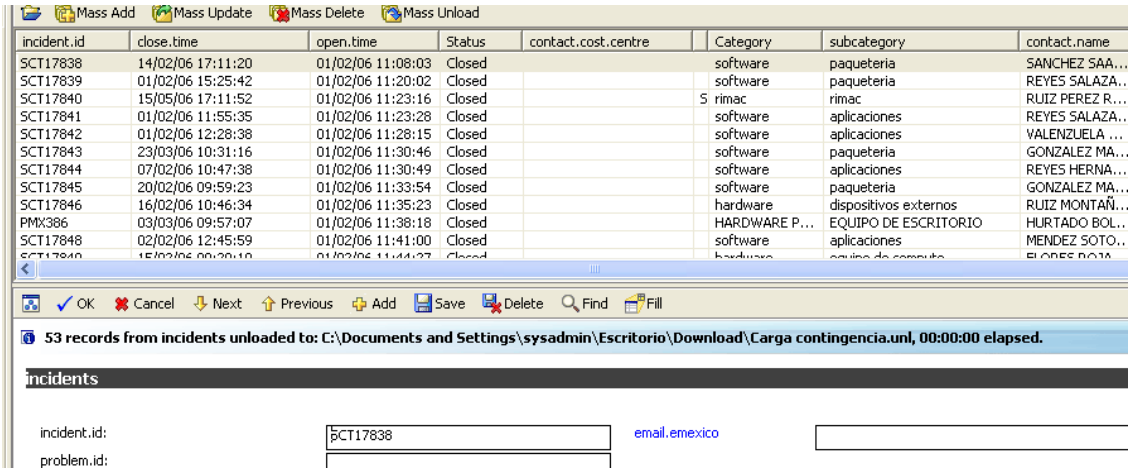
1.4 Dada la lista se que se va a enviar en la opción de mass unload para bajar los registros que se generaron en el lapso que se trabajo con el ambiente de respaldo.





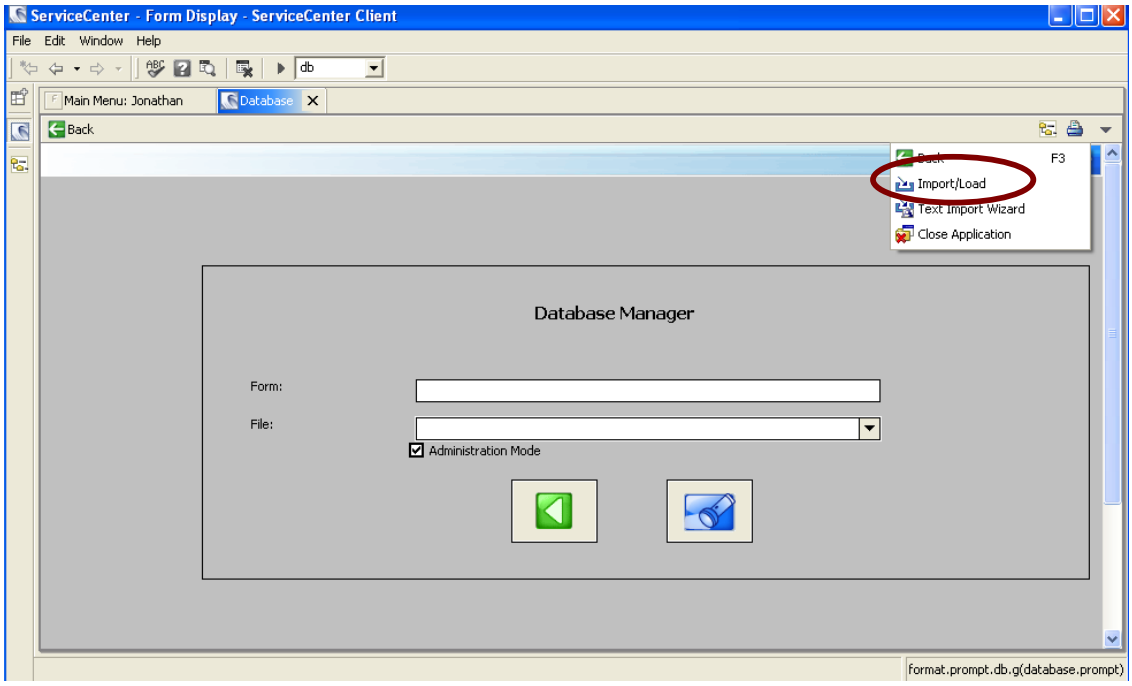
1.5 Todos los file que se exporten pueden exportarse con el mismo nombre para no hacer cargas individuales.

1.6 Una vez descargado el archivo.

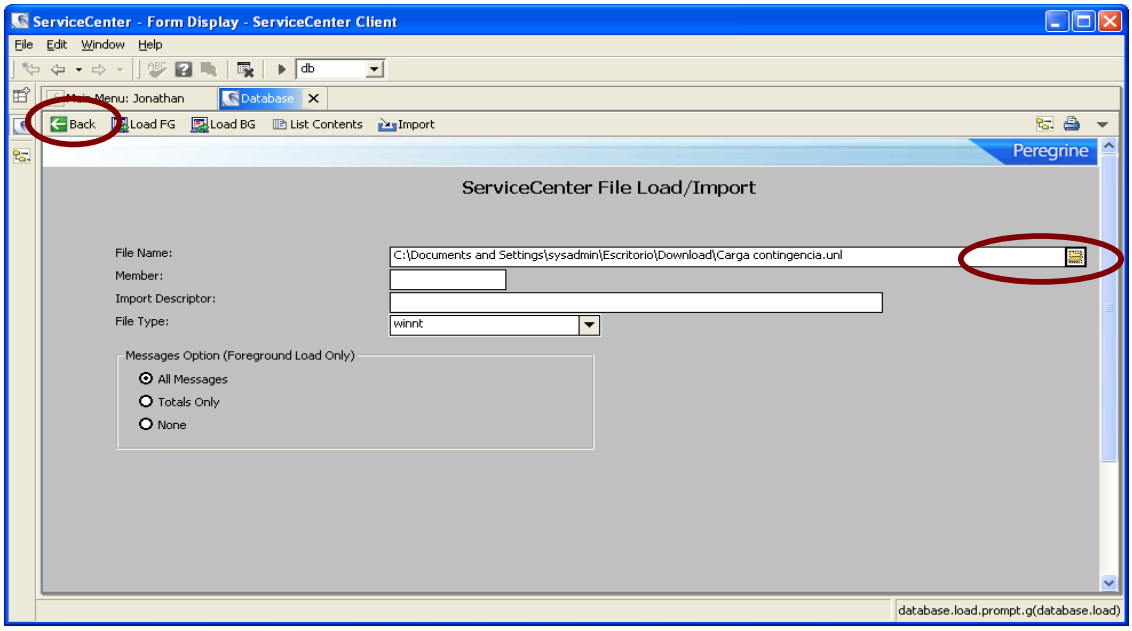


1.7 Dentro del ambiente productivo.

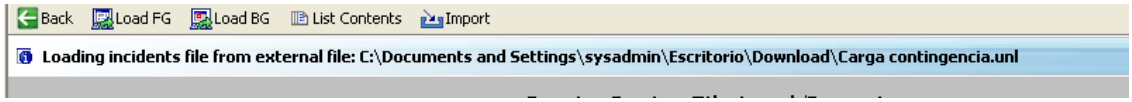
1.8 En el modulo de DB en la opción de import load.

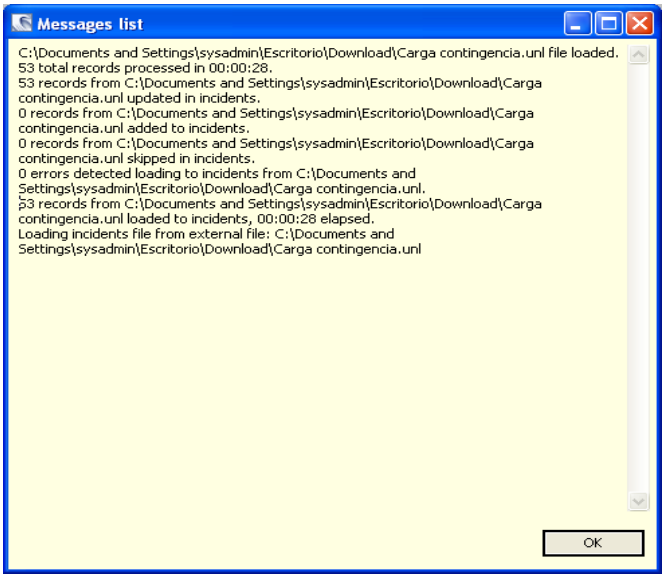


1.9 Seleccionar el archivo desde la ruta que se guardo.



Y cargarlo por medio de la opción de Load FG.





1.10 Al terminar la carga del archivo todos los datos generados en la contingencia serán enviados al ambiente de producción y se pueden manipular y tratar como cualquier dato normal generado en el ambiente de producción

Procedimiento de Restauración

Tiempo de restauración: 5 horas

Acciones:

Se realiza la re-instalación del sistema completo y se recupera la base de datos de Respaldo.

Una vez restaurado y antes de ponerlo en operación nuevamente se integran los datos generados en la instancia de contingencia.

Recomendaciones:

Mantener al día el procedimiento de Plan de Medidas Preventivas BD ServiceCenter.

Conclusiones:

En base al Plan de Contingencia y recomendaciones dadas recuperar el sistema ServiceCenter se obtenga que los niveles de servicio con los clientes estén cubiertos al 99.9%.

Matriz de Pruebas Post-Contingencia:

No	Prueba	Resultado esperado	Firma y Fecha de aceptado
1	Confirmar que los elementos de la Mesa de Servicios puedan levantar llamadas sin problemas.	Levantamiento satisfactorio de llamadas.	
2	Confirmar que los elementos de la Mesa de Servicios puedan levantar incidentes sin problemas.	Levantamiento satisfactorio de incidentes.	

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

F-3 PLAN DE CONTINGENCIA TELEFONÍA

Objetivo:

Describir el procedimiento para recuperar las actividades críticas de operación, en caso de interrupciones parciales o totales por causa de fallas en PBX HiPath 4000, ACD, y/o enlaces de voz, para mantener los servicios de operación al 99%.

Alcance:

- Mesa de Servicios
- Call Center
- NOC

Condiciones para la ejecución del Plan:

Responsabilidad: Este plan deberá ser ejecutado por o bajo la supervisión de los elementos de la Gerencia de Infraestructura y NOC.

Cuando se ejecuta: Se ejecuta cuando se detecta una falla en el envío y recepción de llamadas.

Autorización: No hay pre-autorización para la ejecución, no hay firma de autorización y se levantará reporte en el ServiceCenter.

Notificaciones: Se notifica a la Gerencia de Infraestructura.

Prioridad de Llamada	Tel. 53402700	Nombre	Celular	e-mail
1	a) Teléfono, Nombre, celular, e-mail se eliminan **FUNDAMENTO LEGAL:** Artículo 3 fracción II, 18 fracciones I y II, y 19 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el segundo párrafo del Segundo Transitorio y primer párrafo del Cuarto Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública publicada en el Diario oficial de la Federación el 09 de mayo de 2016, así como en el Lineamiento Trigésimo Octavo, Trigésimo noveno y Cuadragésimo, de los Lineamientos Generales para la Clasificación y Desclasificación de la información de las dependencias y entidades de la Administración Pública Federal publicado en el mismo órgano de difusión el 15 de abril de 2016. **Motivación:** Datos personales y/o datos financieros y/o patrimonial			
2				
3				

Pre-conocimiento**:** Los elementos que ejecuten este plan deberán contar con conocimientos acerca de:
Conceptos medios de Telecomunicaciones:

- Conocimiento básico del Hardware del PBX
- Conocimiento de la distribución de enlaces (E1's de Voz)
- Acceso a ServiceCenter

Material y datos requeridos antes de inicio:

- Ficha técnica del HiPaht 4000
- Último diagrama de configuración
- Detalle de enlaces de voz
- Lista de contactos

Precauciones. Considerar las condiciones de acceso a los siguientes sistemas:

- Acceso restringido al Site de Comunicaciones (deberá tener autorización en el sistema de control de acceso de CEPRA).
- Protección contra electrostática al manipular el Hardware del PBX
- Realizar un checklist previo a la intervención del equipo.
- Contar con el apoyo en sitio o por teléfono de los proveedores especialistas.

Procedimiento:

Monitoreo del comportamiento:

Se aplicara diariamente una rutina de revisión de operación del PBX, revisando la disponibilidad de los servicios de telefonía

Declaración de Emergencia:

Se declara una emergencia cuando se detecta ausencia de llamadas telefónicas en la Mesa de Servicios, Call Center y/o NOC

Procedimiento de Reanudación Enlaces de Voz

Tiempo de Reanudación: 1 hora

Acciones:

Al detectarse que la ausencia de llamadas es debido a problemas con el o los enlaces de Voz hacia el cliente, se procede a configurar en los PBX orígenes un direccionamiento hacia PSTN (Public Switched Telephone Network) que permita que las llamadas generadas dentro de la red telefónica del cliente sean enviadas hacia un número Local o numero 01800 propiedad de CEPRA. A su vez estos DID´s se configuran como entrada en el ACD para que sean dirigidos a los agentes de la Mesa de Servicios, Call Center, y/o NOC.

Equipos y/o Servicios Críticos en el Tiempo.

- Llamadas telefónicas
- Atención a clientes en Mesa de Servicios, Call Center, NOC

Procedimiento de Recuperación Enlaces de Voz

Tiempo de recuperación: Inmediata

Acciones:

Se mantienen la operación de los servicios críticos en el tiempo, se procede a dar seguimiento a los reportes levantados con el carrier.

Equipo y/o Servicios Complementarios

Ninguno

Procedimiento de Restauración Enlaces de Voz

Tiempo de restauración: 24 horas

Acciones:

Restablecido el o los enlaces de voz con el cliente se procede a cancelar el direccionamiento hacia la PSTN (Public Switched Telephone Network) en el PBX del cliente dejando la configuración original permitiendo que las llamadas generadas dentro de la red del cliente se envíen por el medio normal.

Recomendaciones:

Siempre que se implementen enlaces privados entre CEPRA y el cliente habrá que acordar este plan de contingencia para preparar los equipos en ambas puntas y minimizar el tiempo de caída durante cada una de las fases de la contingencia.

Procedimiento de Reanudación ACD (Automatic Call Distributor)

Tiempo de Reanudación: 2- 3 horas

Acciones:

Al detectarse que la ausencia de llamadas es debido a problemas con el ACD , se procede a configurar en el PBX un método de distribución de llamadas básico (Hunting Group) que permita distribuir las llamadas a las extensiones de la Mesa de Servicios, Call Center, y NOC, permitiendo que los agentes sigan atendiendo llamadas.

Equipos y/o Servicios Críticos en el Tiempo.

- Llamadas telefónicas
- Atención a clientes en Mesa de Servicios, Call Center, NOC

Procedimiento de Recuperación ACD (Automatic Call Distributor)

Tiempo de recuperación: Inmediata

Acciones:

No se implementa ninguna acción, se mantienen la operación de los servicios críticos en el tiempo, se procede a dar seguimiento a los reportes levantados con el proveedor de ACD para la recuperación del servidor

Equipo y/o Servicios Complementarios:

Ninguno

Procedimiento de Restauración ACD (Automatic Call Distributor)

Tiempo de restauración: 24 horas

Acciones:

Una vez recuperada la operación y configuración del servidor de ACD se procede a migrar las extensiones configuradas en el "Hunting Group" del PBX hacia el Servidor de ACD

Recomendaciones:

Se tendrá previsto acordar los tiempos de respuesta para este evento con el Proveedor de ACD, manteniendo siempre un respaldo de la configuración última del sistema.

Procedimiento de Reanudación PBX

Tiempo de Reanudación: 24 horas

Acciones:

Al detectarse que la ausencia de llamadas es debido a problemas con el PBX, se procede a implementar un sistema de PBX alterno debiendo contar con al menos 2 tarjetas E1, y manejo de 60 extensiones, se adecuaran las conexiones para los E1's así como para la distribución de de las llamadas mediante un "Hunting Group" a las extensiones de la Mesa de Servicios, Call Center y NOC.

Equipos y/o Servicios Críticos en el Tiempo.

- Llamadas telefónicas
- Atención a clientes en Mesa de Servicios, Call Center, NOC

Procedimiento de Recuperación PBX

Tiempo de recuperación: 12 horas

Acciones:

Se cuenta en almacén con un PBX Panasonic KXT336. Se integran al PBX alterno las extensiones de supervisores y personal operativo que por su importancia directa en el negocio requiera el servicio de telefonía, se mantienen la operación de los servicios críticos en el tiempo, se procede a dar seguimiento a los reportes levantados con el proveedor de PBX para la recuperación del sistema.

Equipo y/o Servicios Complementarios

- Extensiones de Supervisores
- Extensiones de Operaciones

Procedimiento de Restauración PBX

Tiempo de restauración: 72 horas

Acciones:

Una vez recuperado el sistema y configuración del PBX por parte del proveedor, se migraran las conexiones de E1's, extensiones y ACD, que permitan la operación normal de la Mesa de Servicios, Call Center y NOC.

Recomendaciones:

Se tendrá previsto acordar los tiempos de respuesta para este evento con el Proveedor de PBX, manteniendo siempre un respaldo de la configuración última del sistema. Así como la adquisición de un sistema mínimo de PBX con la configuración suficiente para recibir llamadas y distribuirlas a las extensiones.

Conclusiones:

En base al Plan de Contingencia y recomendaciones del sistema telefónico de CEPRA antes descrito se puede concluir que el servicio de atención telefónica está cubierto en un 99%.

Matriz de Pruebas Post-Contingencia:

Establecer las pruebas a realizar una vez superada la contingencia para asegurar que la operación es normal

No	Prueba	Resultado esperado	Firma y Fecha de aceptado
1	Verificar estado de CPU de PBX y tarjetas	CPU, PBX y tarjetas trabajando normalmente	
2	Verificar acceso a número telefónicos locales	Acceso total a números locales	
3	Verificar acceso a extensiones	Acceso total a extensiones	
4	Verificar marcación de extensiones a números locales y largas distancias	Marcación sin problemas	

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE RECUPERACIÓN DE DESASTRES Y PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 27/05/2009	

F-4 PLAN DE CONTINGENCIA ENERGÍA ELÉCTRICA

Objetivo:

Describir el procedimiento para recuperar las actividades críticas de operación, en caso de interrupciones parciales o totales por causa de fallas en el suministro de energía eléctrica comercial, para mantener los servicios de operación al 99.9%.

Alcance:

- Mesa de Servicios
- Call Center
- NOC

Condiciones para la ejecución del Plan:

Responsabilidad: Este plan deberá ser ejecutado bajo la supervisión de la Gerencia de Infraestructura.

Cuando se ejecuta: Se ejecuta cuando se detecta un corte de energía eléctrica comercial.

Autorización: No hay pre-autorización para la ejecución, no hay firma de autorización y se levantará reporte en el ServiceCenter.

Notificaciones: Se notifica a la Gerencia de Infraestructura con el siguiente escalamiento:

Prioridad de Llamada	Tel. 53402700	Nombre	Celular	e-mail
1	**a) Teléfono, Nombre, celular, e-mail se eliminan** **FUNDAMENTO LEGAL:** Artículo 3 fracción II, 18 fracciones I y II, y 19 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el segundo párrafo del Segundo Transitorio y primer párrafo del Cuarto Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública publicada en el Diario oficial de la Federación el 09 de mayo de 2016, así como en el Lineamiento Trigésimo Octavo, Trigésimo noveno y Cuadragésimo, de los Lineamientos Generales para la Clasificación y Desclasificación de la información de las dependencias y entidades de la Administración Pública Federal publicado en el mismo órgano de difusión el 15 de abril de 2016. **Motivación:** Datos personales y/o datos financieros y/o patrimonial			
2				
3				

Pre-conocimiento. Los elementos que ejecuten este plan deberán contar con conocimientos acerca de:

- Conceptos básicos de electricidad.
- Ubicación de la infraestructura eléctrica (tableros de control del Site del CEPRA, UPS y planta de emergencia)
- Acceso al sistema de seguimiento de ServiceCenter (bitácora).

Material y datos requeridos antes de inicio:

- Lista de contactos de proveedores
- Memoria técnica del sistema eléctrico (disponible en la biblioteca del NOC)
- Procedimiento de medidas preventivas Sistema Eléctrico
- Contraseña de acceso al sistema ServiceCenter.

Precauciones. Considerar las condiciones de acceso a los siguientes sistemas:

- UPS. Acceso restringido al Site de Comunicaciones (deberá tener autorización en el sistema de control de acceso de CEPRA)
- Planta de emergencia. Considerar las condiciones de acceso tanto para la revisión y/o supervisión como para la carga de combustible (diesel).

Procedimiento:

Monitoreo del comportamiento:

El operador del NOC tendrá permanentemente monitoreado el UPS a través del software LanSafe, instalado en los equipos de operación, apegado al Plan de Medidas Preventivas para el Sistema de Suministro Eléctrico.

Declaración de Emergencia:

- Se declara una emergencia eléctrica en el momento que se presenta un fallo o corte en el suministro eléctrico comercial.
- Se apagará el alumbrado del inmueble de CEPRA que está soportando al tablero que recibe la energía comercial.
- Comienzan acciones estipuladas en el procedimiento de reanudación.

Procedimiento de Reanudación

Tiempo de Reanudación: Inmediato

Acciones:

Al detectarse la ausencia de suministro eléctrico comercial a la entrada del sistema de UPS, este activa el sistema de baterías para seguir manteniendo la salida del UPS con el nivel de voltaje y corriente Normales, alimentado todos los equipos conectados al tablero de emergencia:

Equipos y/o Servicios Críticos en el Tiempo:

- Equipos de Comunicaciones y Red
- Servidores
- PBX
- Estaciones de Trabajo de Mesa de Servicios, Call Center, NOC
- Estaciones de Trabajo Supervisión, Gerencia, Dirección y administrativos

- Equipos de Acceso Biométrico
- Video Vigilancia
- Alumbrado de Emergencia
- Pantallas de monitoreo

Procedimiento de Recuperación

Tiempo de recuperación: 10 segundos

Acciones:

Tras la detección del fallo en el suministro eléctrico comercial y la activación del banco de baterías del UPS, se enciende el motor de la planta de emergencia que generara la energía eléctrica suficiente para sustituir el suministro eléctrico comercial a la entrada del UPS con esto el UPS regresa a su función de regulación y recarga de baterías, se mantiene la alimentación eléctrica en los componentes mencionados en el procedimiento de reanudación y adicionalmente se recupera la alimentación en:

Equipo y/o Servicios Complementarios:

- Sistema de Climatización del Site de Comunicaciones
- Alumbrado General

Procedimiento de Restauración

Tiempo de restauración: Variable

Acciones:

Se restablece el suministro eléctrico comercial, el UPS detecta a la entrada el suministro de energía, se desactiva la operación de la planta de emergencia, y se vuelve a la operación normal.

Recomendaciones:

Debido a que la infraestructura del CEPRA está ubicada en una zona de negocios (Av. Insurgentes) donde se presenta una alta demanda de energía, los cortes de energía comercial son constantes, aumenta su periodicidad de fallas (cortes de energía más constantes) en la época de lluvias (julio-octubre). Debido a este problemática es necesario una revisión periódica (cada 15 días) de la cantidad de combustible de la planta de emergencia.

El límite recomendado es que el depósito de almacenamiento de combustible (diesel) debe estar al 85 % (aproximadamente 85 litros), máxima capacidad es de 100 litros.

Conclusiones:

Con base al Plan de Contingencia y recomendaciones del sistema eléctrico del CEPRA antes descrito se puede concluir que los Sistemas de Operación (Aplicaciones de producción tanto del CEPRA como de sus clientes) y los Servicios internos (Internet, LAN, sistema telefónico, iluminación) están cubiertos en un nivel de Servicio del 99.9 %

Matriz de Pruebas Post-Contingencia:

No	Prueba	Resultado esperado	Firma y Fecha de aceptado
1	Confirmar que la entrada de UPS es suministro comercial	Niveles de Voltaje medidos en la entrada de UPS reportados en LAN Safe.	
2	Confirmar apagado de Planta de emergencia	Planta de emergencia apagada con métricas del panel de control normales.	
3	Operación de la totalidad de equipos y luminarias	Se confirma la operación de equipos con suministro eléctrico regulado y no regulado (PC, Laptops, impresoras, etc.).	

PRUEBAS AL PLAN DE CONTINUIDAD DEL NEGOCIO

Políticas:

- Las pruebas para determinar la efectividad y funcionamiento total del Plan de Continuidad del Negocio (BCP) se realizarán al menos una vez al año.
- Cuando la Dirección de CEPRA lo considere necesario, podrán realizarse pruebas parciales sobre algún servicio o elemento en específico, esta excepción deberá estar documentada.
- La calendarización de las pruebas al BCP será definida por la Dirección General de CEPRA, considerando la paralización parcial del negocio; el día estará designado en función de la carga laboral.
- La simulación de eventualidades estará a cargo del área de Infraestructura de CEPRA.
- Todas las observaciones y notas producto de estas pruebas deberán ser registradas y difundidas a la alta Dirección.
- El tratamiento de vulnerabilidades u oportunidades de mejora serán coordinadas por el área de Infraestructura y tratadas por los responsables pertinentes.

Pruebas Realizadas al Plan de Continuidad del Negocio

A continuación se adjunta el resultado del último evento simulado realizado en CEPRA y como parte del cumplimiento con las disposiciones internas respecto al Plan de Continuidad de Negocio.

El evento consistió en simular un apagón, para lo cual el área de Infraestructura cortó el suministro de energía eléctrica el día jueves 6 de Noviembre del 2008 a las 16:00 horas, reestableciendo el servicio a las 16:35hrs; durante el tiempo que fue cortada la energía eléctrica, se realizaron diversas pruebas para comprobar el estado de algunos componentes de infraestructura que soportan la prestación de servicios de CEPRA ante la eventualidad simulada.

El resultado del registro de las pruebas es el siguiente:

No	Prueba	Resultado Obtenido	Nombre	Puesto	Firma
	Red de Datos				
1	Probar conectividad entre equipos	Conectividad positiva entre equipos	a) Eliminado	Gte. Infraestructura	b) Eliminado
2	Probar accesos a servicios de red	Accesos posibles a los diversos servicios de red como fueron: impresoras compartidas, internet y archivos compartidos		Gte. Infraestructura	
	Service Cen				
1	Confirmar que los elementos de la mesa de servicio puedan levantar llamadas sin problemas.	Se observó que no hubo afectación para poder recibir y atender llamadas por parte de la Mesa de Servicio.		Gte. Infraestructura	
2	Confirmar que los elementos de la mesa de servicio puedan levantar incidentes sin problemas.	No se registró ningún problema al momento de levantar incidentes reportados por los clientes.		Gte. Infraestructura	
	Telefonía				
1	Verificar estado de CPU de PBX y tarjetas	Tarjetas y CPU on-line		Ing. Soporte	
2	Verificar acceso a número telefónicos locales	Se comprobó que todos los teléfonos permitieron marcar números telefónicos locales		Ing. Soporte.	
3	Verificar acceso a extensiones	El acceso a las extensiones fue positivo		Ing. Soporte.	
4	Verificar marcación de extensiones a números locales y largas distancias	Se tomó una muestra de 5 extensiones de diferentes áreas y de todas se pudieron establecer llamadas a números telefónicos locales y de larga distancia		Ing. Soporte.	
	Energía Eléc				
1	Confirmar que la entrada de UPS es suministro comercial	212 Volts		Ing. soporte.	
2	Confirmar apagado de Planta de emergencia	Planta de emergencia apagada una vez solucionada la eventualidad		Ing. soporte.	
3	Operación de la totalidad de equipos y luminarias	Se confirmó la operación íntegra de equipos con suministro eléctrico regulado y no regulado (PC, Laptops, impresoras, etc.).		Ing. Soporte.	

Resultado de las pruebas al Plan de Continuidad del Negocio

a) Nombre,b) firma
FUNDAMENTO LEGAL: Artículo 3 fracción II, 18 fracciones I y II, y 19 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el segundo párrafo del Segundo Transitorio y primer párrafo del Cuarto Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública publicada en el Diario oficial de la Federación el 09 de mayo de 2016, así como en el Lineamiento Trigésimo Octavo, Trigésimo noveno y Cuadragésimo, de los Lineamientos Generales para la Clasificación y Desclasificación de la información de las dependencias y entidades de la Administración Pública Federal publicado en el mismo órgano de difusión el 15 de abril de 2016.
Motivación: Datos personales y/o datos financieros y/o patrimonial

AFN - Plan de Anticipación de Fenómenos Naturales

PLAN DE ANTICIPACIÓN DE FENÓMENOS NATURALES

Objetivo

El presente Plan de Anticipación de Fenómenos Naturales tiene como razón de ser los siguientes objetivos:

1. Conocer y difundir las buenas prácticas de salvaguarda del personal e información crítica para el negocio.
2. Mantener evidencia de los elementos y actividades necesarias que CEPRA ha definido como parte de las acciones necesarias para participar proactivamente ante la manifestación de fenómenos naturales.

Introducción

La ocurrencia de fenómenos naturales en nuestro país es alta y en muchas ocasiones estos fenómenos naturales derivan en desastres que traen consigo impactos financieros a las empresas del país; es por esto que se debe estar preparado para que los impactos de cualquier desastre natural no sean graves al negocio.

El presente plan incorpora buenas prácticas que deben ser consideradas al manifestarse un fenómeno natural que pueda traer consigo una situación de desastre.

Lo descrito en este plan sirve como base inicial ante una posible activación del plan de TI de recuperación de desastres.

Invocación

El Plan de Anticipación de Fenómenos Naturales, sólo podrá ser activado cuando se vean amenazados los recursos humanos y/o la infraestructura de CEPRA, los responsables de activar este plan son:

- Director General de CEPRA
- Director de Infraestructura

Lineamientos Generales

- La activación de este plan sólo puede ser determinada por los cargos descritos en el apartado "Invocación".
- El presente plan deberá ser revisado y adecuado a las necesidades y características del negocio cada 6 meses.

- Las pruebas a la efectividad del plan de recuperación se deben realizar en su totalidad al menos una vez al año. Durante las pruebas se deberá verificar la funcionalidad de los planes de contingencia del plan, la respuesta a la emergencia.

- Este documento deberá ser resguardado en electrónico y en físico en algún sitio alterno que disponga la Dirección General, así mismo, la ubicación que se determine deberá ser del conocimiento del equipo de recuperación.

- El área de Infraestructura será la responsable de la custodia de este documento y de los demás documentos relacionados a este plan.

Acciones

Con base al análisis de riesgos desarrollado por CEPRA, los posibles fenómenos naturales a los cuales se está expuesto son:

- Inundaciones catastróficas
- Sismos

Ante inundaciones catastróficas se debe:

1. Todo el personal de CEPRA debe seguir las indicaciones que la Brigada de evacuación dictamine para trasladarlos a un lugar seguro (Consultar guía de evacuación).

2. El Gerente de Infraestructura deberá tener a la mano las llaves maestras de acceso a los espacios físicos en los cuales se encuentran los componentes críticos que soportan la operación de los servicios de TI y las llaves de acceso de los espacios en los que se tienen almacenados los respaldos de información y datos de los servicios de TI que se proveen.

3. De ser posible, el Gerente de Infraestructura o su respaldo deberán cerrar todas las instalaciones de CEPRA asegurándose de que ningún personal quede atrapado en ellas.

4. Los directivos de CEPRA con base en la magnitud del desastre determinarán la activación inmediata del plan de recuperación de desastres para garantizar la operación de los servicios de TI que se proveen.

5. Una vez que transcurra el desastre natural (inundación) o cuando las autoridades así lo permitan, el equipo de recuperación ingresará a las instalaciones para evaluar y restaurar los daños ocurridos.

6. Restaurada la infraestructura, contactar al personal de CEPRA para el reinicio de operaciones.

Ante un sismo se debe:

1. Todo el personal de CEPRA debe seguir inmediatamente las indicaciones que la Brigada de evacuación dictamine para trasladarlos a un lugar seguro (Consultar guía de evacuación).

2. El Gerente de Infraestructura deberá tener a la mano las llaves maestras de acceso a los espacios físicos en los cuales se encuentran los componentes críticos que soportan la operación de los servicios de TI y las llaves de acceso de los espacios en los que se tienen almacenados los respaldos de información y datos de los servicios de TI que se proveen.

3. Los directivos de CEPRA con base en la magnitud de los daños ocasionados por el desastre, determinarán la activación inmediata del plan de recuperación de desastres para garantizar la operación de los servicios de TI que se proveen.

4. Cuando las autoridades así lo permitan, el equipo de recuperación ingresará a las instalaciones para evaluar los daños ocurridos, rescatar al personal atrapado y retirar la información del negocio que sea necesaria para continuar con las operaciones del mismo.

5. Iniciar actividades de restauración de manera inmediata.

6. Restaurada la infraestructura, contactar al personal de CEPRA para el reinicio de operaciones.

Dependencias

En adición a la activación de este plan, es necesario que se disponga de los siguientes documentos:

- Guía de evacuación

PLAN DE CONTINUIDAD DEL NEGOCIO	Código: CE-PN-RS-01	
	Versión: 01	Revisión: 01
	Fecha Efec: 12/01/2009	

GUÍA DE EVACUACIÓN

Concepto:

Evacuación.- Es la acción de desocupar de manera ordenada y planificada un lugar. Esta acción o desplazamiento es realizado por los ocupantes y por razones de seguridad ante un peligro potencial o inminente.

Lineamientos:

- El concepto de evacuación también incluye el desplazamiento de los bienes y documentos (valores, etc.) que se considere de vital importancia o que sean irrecuperables ante un evento que se presente o afecte a las instalaciones de la empresa.
- La ubicación y plena visibilidad de las señales de evacuación serán revisadas semestralmente, en caso de que se les tenga que hacer algún tipo de mantenimiento, este deberá ser realizado de manera inmediata.
- La evacuación rápida y oportuna es una forma de evitar pérdidas, por lo que se requiere que sea una actividad organizada por parte del personal de CEPRA.
- En apego al carácter preventivo de este documento, se deberá hacer al menos un ejercicio anual de evacuación de todo el personal de CEPRA

Casos en que debe realizarse la evacuación:

Debido a la posición geográfica de CEPRA y con base en el análisis de riesgos desarrollado, los fenómenos naturales a los que está expuesta son:

- Sismos.
- Inundaciones catastróficas

Nota: La evacuación también podrá realizarse cuando así lo determinen las autoridades ante alguna situación de amenaza que no precisamente sea de carácter natural, como pueden ser atentados, amenaza de bomba o sus derivados.

Responsables:

- Jefe de Evacuación (Coordinador de Emergencia)
- Jefes de Brigadas (Evacuación y Primeros Auxilios)

Responsabilidades:

Jefe de Evacuación (Coordinador de Emergencia):

- Asume la dirección y el control de toda la operación de evacuación de CEPRA.
- Coordina el apoyo con dependencias externas tales como Bomberos, Policías y Cuerpos de Emergencia.
- Organiza y coordina la capacitación a las brigadas necesarias.
- Organiza sistemas de control y chequeo para época normal y de emergencia, de los medios y recursos para la operación.

Jefes de Brigada:

- Asumen la acción correspondiente a su tarea específica.
- Coordinan entre sí para evaluar la acción y la distribución de tareas específicas.
- Organizan y mantienen entrenado a todo su personal en las tareas de la brigada correspondiente.
- Emiten sugerencias al Jefe de Evacuación, con base en las observaciones y experiencias recogidas.

Personal en general:

- Facilitarán las acciones del Jefe de Evacuación, actuando conscientemente en función de este plan.
- Obedecerán las disposiciones e indicaciones de las brigadas y/o de sus Jefes de acción, cumpliendo las reglas de seguridad y evacuación.
- Adoptarán un comportamiento adecuado de mutua ayuda física y psicológica durante los simulacros y ante una situación real.
- No usarán los teléfonos para llamada familiares durante una emergencia.
- Conservarán las clasificaciones, restricciones y sus emplazamientos.
- Se conducirán de manera correcta y con plena seriedad durante los simulacros que se realicen.

Acciones:

Durante una situación de emergencia y/o simulacro, las acciones a realizar son las siguientes:

Jefe de Evacuación

1. Notifica la acción de evacuación a todo el personal de CEPRA.
2. Da a conocer el tipo de emergencia a los Jefes de Brigada.

Jefe de Evacuación y Brigada de Evacuación

3. Desaloja a los visitantes y a todo el personal de las instalaciones de CEPRA.
4. Se asegura de que todo el personal evacue las instalaciones de CEPRA.
5. Canaliza al personal al punto de reunión o área segura establecida.

Brigada de primeros auxilios:

6. Dentro del área segura, auxilia médica y psicológicamente al personal afectado en una primera instancia.

7. Identifica a los heridos y emite reporte respecto al estado de salud.

8. El Jefe de la brigada de primeros auxilios debe registrar a detalle los lugares de atención y condiciones físicas a los que son trasladados los heridos.

Jefe de Evacuación

9. Decide en conjunto con el Director de Infraestructura y las autoridades necesarias el reingreso del personal a las instalaciones de CEPRA.

10. En caso de que no se permita el acceso a las instalaciones, se deben considerar las acciones dispuestas en el plan de recuperación de desastres.

Comunicación:

Alarma:

- CEPRA cuenta con megáfono o "alta-voz" mediante el cual se difunden los mensajes e instrucciones al personal para realizar las acciones requeridas para la evacuación del personal.