UNIVERSIDAD DE LAS AMÉRICAS

FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

Plan de Continuidad de Negocios en el Área de TI

Trabajo de Titulación presentado en conformidad a los requisitos
establecidos para optar por el título de:
Ingeniera en Sistemas de Computación e Informática

Profesora Guía:
Ing. Mayrita Valle

AUTORA:
GRACE ELIZABETH SALAZAR LÓPEZ

Año
2012

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Mayrita Valle
Ingeniera en Sistemas
C.I.: 0601583020-3

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Grace Elizabeth Salazar López

C.I.: 171331019-9

AGRADECIMIENTOS

Mis más sinceros agradecimientos a Israriego por su aval brindado en toda mi carrera. Gracias a mi madre y hermana porque siempre confiaron en mis capacidades, gracias por su apoyo incondicional. Gracias a mi esposo por su paciencia y por su ejemplo de dedicación y amor. Y sobre todas las cosas Gracias mi Dios porque en tu infinito amor cumpliste los anhelos de mi corazón.

DEDICATORIA

En toda mi vida has estado conmigo Señor, aún cuando no advertí que estabas ahí, estuviste cubriéndome y cuidándome con amor de Padre, eres el principal ser a quien dedicaré toda mi vida y esta etapa en especial, has sido mi patrocinador, mi gestor financiero, mi consejero y entre tantas otras cosas mi ayudador incondicional. A ti Señor mi principal dedicación.

A mi esposo quien me ha impulsado a terminar este largo camino con su compresión, amor y ayuda hasta en los más pequeños detalles.

A mi madre por ser ejemplo de lucha y fortaleza, por dedicar su vida a sus hijas.

Grace Salazar

RESUMEN

Este trabajo se realizó con el propósito de proporcionar un plan de continuidad de negocios para la empresa Israriego Cía. Ltda., en base a métodos y análisis bajo estándares internacionales.

Se realizó un estudio de la situación actual de la empresa para proponer el plan a seguir y demostrar la importancia del desarrollo del plan de continuidad de negocios.

Se efectuó el plan de trabajo y se presentó a los directivos de la empresa quienes receptaron la propuesta de forma positiva y accedieron a colaborar en el desarrollo del plan reconociendo su beneficio tanto a corto como a largo plazo.

Se procedió a realizar el análisis del impacto al negocio para lo cual se determinó la cadena de valor en los procesos y se determinaron 3 áreas y procesos específicos de mayor importancia en el negocio, en base a esta primera actividad se realizó el análisis del impacto al negocio así como su estrategia de recuperación.

Por último se levantó la documentación necesaria para realizar las pruebas y mantenimiento del plan, así como toda la documentación como formatos para directrices en los eventos de crisis y cada paso a seguir dentro del proceso de continuidad. Adicionalmente se documentan formularios de prueba y de certificación para lograr altos niveles dentro de futuras auditorías internas.

Por lo tanto este desarrollo ha documentado que es posible reaccionar de manera proactiva ante los eventos que atenten contra la continuidad de los procesos de Israriego.

ABSTRACT

This thesis work was done with the purpose of providing a business continuity plan based on analysis methods and international standards for the company Israriego Cia. Ltda.

A study of the current situation of the company to propose a plan to follow and demonstrate the importance of developing the business continuity plan.

A work plan was done and presented to the directives of the Company who received the proposal and agreed to collaborate in the development of recognizing their benefit plan both short and long term.

We proceeded to perform business impact analysis for which we determined the value chain processes and identified 3 areas and processes of major importance in the business, based on this first activity was held to analyze the impact business as well as its recovery strategy.

Finally, was made the documentation needed for the testing and maintenance of the plan and documentation will all guidelines and formats for crisis events and each next step in the process of continuity. Additionally, test forms and document certification to achieve high levels in future internal audits.

Therefore, this development has been documented that it is possible to proactively react to events that threaten the continuity of Israriego processes.

ÍNDICE

INDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Hoy en día se reconoce que la “Planificación de Continuidad de Negocio” y planificación de recuperación ante desastres son actividades vitales; sin embargo, la creación y mantenimiento de una continuidad de las actividades y un plan de recuperación de desastres, es una tarea compleja, que implica estudio y análisis.

Antes de la creación del plan en sí mismo, es esencial considerar los posibles impactos de los desastres y comprender los riegos subyacentes, a partir de estas actividades el plan en si mismo debe construirse; el Plan de Continuidad de Negocios o sus siglas en inglés “BCP – Business Continuity Plan” debe tener control y auditoría para garantizar que sigue siendo apropiado a las necesidades de la organización.

El BCP está diseñado para considerar todas estas necesidades, el primer paso en un proceso de continuidad de negocios es considerar los posibles impactos de cada tipo de desastre o evento.

Esto es crítico ya que ¿Cómo se puede planificar adecuadamente para un desastre si no poseemos idea de los posibles impactos en la empresa u organización de los distintos escenarios?

Una vez determinados los impactos, se debe considerar con la misma importancia la magnitud de los riesgos que podrían dar lugar a estos. Esta es una actividad crítica que determinará los escenarios y su ocurrencia por lo que debería revisarse a conciencia durante el proceso de planificación.

Para la empresa Israriego la toma de decisiones está basada en la información recopilada con el transcurso de su historia del negocio, todos los datos tales como Estadísticas de venta, cartera, información de clientes proveedores y

empleados hacen que la información se de vital importancia para sus decisiones gerenciales.

Es por esta razón que Israriego desea implementar dentro de sus procesos un plan de continuidad de negocios en lo referente a información y posteriormente en todas sus áreas de negocio.

El presente estudio desarrollará un Plan de Continuidad de Negocios aplicando el Sistema de Gestión de Seguridad de Información, como resultado se obtendrá recomendaciones de control de seguridad, direcciones para mitigar riesgos, indicaciones especìficas para generar roles y actividades en caso de desastre, emisión de documentación de control, conocimiento de medidas oportunas para mantener riesgos bajo control.

Con los resultados mencionados la organización estará lista para someterse a procesos de auditoría y de evaluación de seguridad de información.

CAPITULO I

En este capítulo se presentará la justificación, los objetivos y el alcance del proyecto, también una descripción general de la empresa Israriego Cia. Ltda., en donde se desarrollara el plan de Continuidad de Negocios en el área de TI.

1 GENERALIDADES

1.1 JUSTIFICACIÓN

Decisiones críticas tomadas en momentos de crisis tienen un alto riesgo de equivocaciones costosas e ineficaces, es así cuando en momento de catástrofe o crisis una entidad o empresa está obligada a continuar con sus actividades cotidianas.

Frente a la probabilidad de ocurrencia de un corte en la continuidad del negocio el problema que enfrentan los departamentos es qué hacer cuando sus localidades quedan inhabilitadas

El objetivo es restaurar las operaciones del negocio en los tiempos y puntos de recuperación establecidos según la necesidad de la organización.

La metodología BCP “Business Continuity Plan” o “Plan de Continuidad de Negocios” es escalable para una organización de cualquier tamaño y complejidad. A pesar de que la metodología tiene sus raíces en las industrias reguladas, todo tipo de organización puede crear un manual de BCP, y podría decirse que cada organización debe tener el fin de garantizar la longevidad de la organización. Un manual de BCP para una organización pequeña puede ser simplemente un manual impreso almacenado de forma segura lejos del lugar principal de trabajo, que contiene los nombres, direcciones y números de teléfono para el personal de gestión de crisis, los miembros del equipo general,

clientes y proveedores junto con la ubicación de la datos fuera del sitio de almacenamiento de copia de seguridad, los medios de comunicación, copias de contratos de seguros, y otros materiales críticos necesarios para la supervivencia de la organización.

Un manual BCP proponer un centro de operaciones alterno en caso de crisis, los requisitos técnicos, los requisitos reglamentarios de presentación de informes, las medidas de trabajo de recuperación, los medios para restablecer los registros físicos, los medios para establecer una nueva cadena de suministro, o los medios para establecer nuevos centros de producción. Las empresas deben asegurarse de que su manual BCP es realista y fácil de usar durante una crisis.

Israriego como tantas otras entidades del Ecuador no poseen un plan de continuidad de negocios, sin embargo desea mantener su negocio activo y con el menor tiempo posible de cortes en su actividad.

Toda empresa se enfrenta a eventos que amenacen el desarrollo de su actividad principal, por lo tanto es importante contar con planes de contingencia existentes que garanticen la continuidad de los negocios por medio de medidas preventivas y estrategias de recuperación de su actividad principal.

Un Plan de Continuidad de Negocios representa un costo relativamente bajo en comparación con lo que la empresa podría perder en un incidente mayor; por tanto, parece más prudente que las organizaciones de todos los tamaños tomen en serio la investigación y el desarrollo de un plausible y eficaz BCP.

1.2 OBJETIVOS

1. Preparar a la organización para manejar efectivamente una situación de desastre que impacte significativamente su capacidad para operar.

2. Definir estrategias, acciones y procedimientos para validar los procesos de recuperación de las operaciones críticas de la organización.

3. Definir los eventos que pudieran tener un impacto material negativo en la organización.

4. Definir cómo responder y reanudar las funciones críticas de negocio y servicios esenciales dentro de la organización.

5. Definir acciones de guía sujetas a validación efectiva del plan de continuidad de negocios.

6. Tomar decisiones mucho antes de que ocurra una contingencia real.

1.3 ALCANCE

Se pretende desarrollar un Plan de Continuidad de Negocios dirigido hacia el área de Tecnología de la Información, que incluye servidores, comunicaciones y continuidad de disponibilidad de información a través de:

- Establecer un plan de respuesta a crisis
- Evaluación de riesgos
- Plan de comunicación de crisis
- Plan de recuperación
- Plan de reanudación de negocios
- Definición de plan de grupos de trabajo, responsables asignados.

Levantar información y formatos para la realización de pruebas y validaciones del plan de continuidad de negocios así como los pasos necesarios para realizar la certificación del plan.

1.4 ANTECEDENTES DE LA EMPRESA

Israriego es la empresa líder en Sistemas de Riego en la Región Andina, es con sede en Israel, cuenta con sucursales en Guayaquil y sus filiales en Perú y Colombia, así como su fábrica de Mangueras de PE y Tubos de PVC donde reside su mayor lugar de producción.

Israriego diseña y produce sistemas de riego, provee insumos y tecnología agroindustrial de procedencia israelí para el mercado Ecuatoriano y la región Andina, ofrece la más avanzada tecnología de riego con avances de punta, debidamente probados para las condiciones que requiere cada cultivo, incluyendo equipos de riego adecuados para regar eficientemente cultivos florícolas, hortícolas, frutales, entre otros, tanto bajo invernaderos como en la intemperie en distintos medios y sustratos. Fabrica e importa materiales y accesorios para sistemas de riego, agua potable, construcción, industria, y todo tipo de infraestructura hidráulica.

Israriego fue fundada en el Ecuador hace dos décadas, se diferencia por su constante exigencia y aspiración a la excelencia, tanto en la calidad de sus productos como en el servicio brindado al cliente.

La empresa cuenta con alrededor de 127 empleados y una amplia lista de distribuidores en todo el Ecuador.

1.4.1 Misión

Ofrecer en la Región Andina la más avanzada tecnología de riego con avances de punta debidamente probados para las condiciones que requiere cada cultivo, incluyendo equipos de riego adecuados para regar eficientemente cultivos florícolas, hortícolas, frutales, entre otros, tanto bajo invernaderos como en la intemperie en distintos medios y sustratos.

1.4.2 Visión

Ser la empresa líder en la comercialización, implementación, uso de la tecnología de punta y servicio en el sector floricultor, cumpliendo con los estándares de calidad y desarrollo sostenible, soportados en estrategias efectivas creadas por colaboradores con talento y visión.

1.5 ESTRUCTURA DE NEGOCIO

Israriego trabaja con las siguientes líneas de venta:

1 Sistemas de riego: Desarrollo e instalación de Sistemas de irrigación por goteo en agricultura, floricultura, jardines, etc.

2 Repuestos: Venta de repuestos en el área de riego, productos importados desde Israel.

3 Plástico: Comercialización y asesoría de plástico israelí para invernadero, mallas.

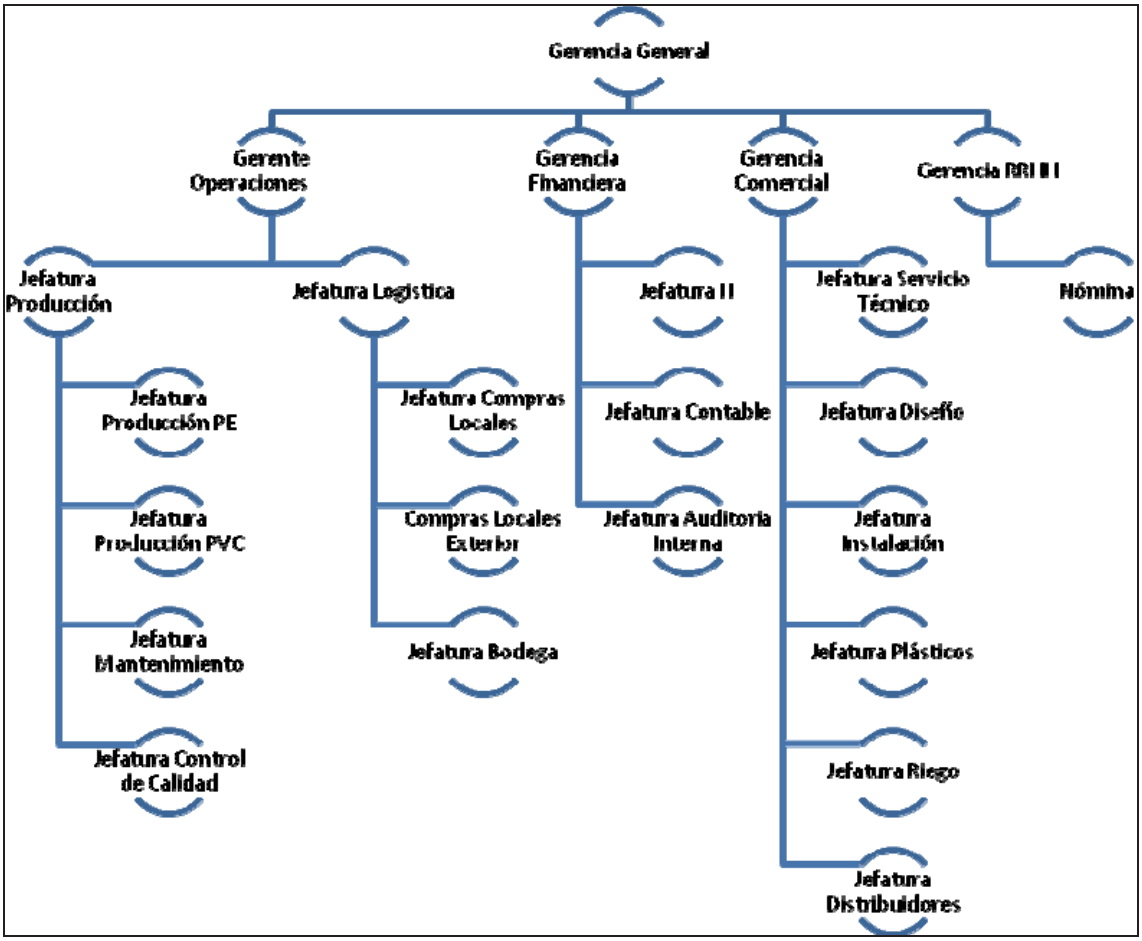
4 Semillas: Venta de semillas como servicio adicional para el cliente de agricultura.

5 Fabrica: Comercialización y fabricación de mangueras y tubería para riego con estándar ISO 9000 e ISO 9001.

6 Distribuidores: Israriego cuenta con 20 distribuidores alrededor de todo el país para venta de productos de riego como manguera, tubería, repuestos, plásticos y semillas, exceptuando el área de servicio sobre Sistemas de riego

1.6 ORGANIZACIÓN DE LA EMPRESA

Figura 1.1: Organigrama de la Empresa Israriego Cia. Ltda.



Fuente: Departamento de Auditoría de la Empresa Israriego Cia. Ltda

CAPITULO II

2 MARCO TEÓRICO

Comprende los siguiente pasos a seguir en las fases del Plan de Continuidad de Negocios, de esta forma se dá a conocer concepto e importancia del BCP.

2.1 CONCEPTO DE BCP

Plan de Continuidad de negocios o sus siglas en Inglès BCP (Business Continuity Plan) también denominado como:

BCP: Business Continuity Plan
BCP: Business Contingency Plan
DRP: Disaster Recovery Plan
CP: Contingency Plan
BRP: Business Recovery Plan
BCM: Administración Continuidad Negocio
SGCN: Sistema de Gestión de Continuidad de Negocios
BCP es un conjunto de acciones a ser llevadas a cabo ante distintos escenarios de desastres que pudieran afectar la correcta marcha de los negocios.[1]

Para un desarrollo efectivo del BCP es necesario llevar a cabo las fases secuenciales y ordenadas del plan.

Para empezar es imperativo conocer la compañía: productos o servicios, objetivos empresariales, procesos y procedimientos internos. Es necesario entender y conocer la razón de ser de la empresa debido a que en base a este

[1] Syed Akhtar, Syed Bmath Afsar, Business Continuity Planning Methodology, 2004.

conocimiento se identificarán los procesos críticos y la prioridad de los procesos a recuperarse en caso de imprevistos de indisponibilidad o desastres.

2.1.1 Propósito del BCP

El propósito del BCP es proteger cuatro puntos escenciales; personal, operaciones, información y la empresa.

Se protegen estos puntos; tomando decisiones efectivas en tiempos de crisis, reduciendo la dependencia de personal específico, minimizando la pérdida de datos, utilidades y clientes, recuperando oportunamente las operaciones, manteniendo la imagen pública y la reputación.

2.2 DESARROLLO DEL PLAN

Se establecen miembros del proyectos tales como: Gerente del proyecto y alcance de sus responsabilidades, se detallan objetivos, metas y resultados finales.

2.2.1 Alcance de Responsabilidades

La primera medida a tomar es elegir al Coordinador de BCP, es necesario que conozca: sus responsabilidades, objetivos, fases, resultados y medidas del proyecto.

El documento del alcance de responsabilidades debe detallar lo siguiente:

- Posición en el equipo y fecha de validez.
- La persona a quien reporta.
- Niveles de autoridad para cuestiones operativas y financieras.
- Niveles de recursos requeridos por la posición.
- Estructura del proyecto.

- Responsabilidades para la evaluación de riesgos e impacto.
- Responsabilidades para preparar y probar el plan.
- Entregables del proyecto.
- Responsabilidades en caso de emergencias.
- Tareas en entrenamiento y mantenimiento.

2.2.2 Selección del Equipo de Trabajo

El director del proyecto y coordinador deberán inicialmente realizar el proceso de selección de personal para los miembros del equipo del proyecto. El objetivo del equipo principal es proporcionar orientación general al equipo, estos deben pertenecer a niveles de gerentes es decir de alto nivel. Es preferible que los miembros principales del equipo pertenezcan a la organización. Este equipo debe ser cuidadosamente seleccionado. Debe existir un representante de cada una de las principales áreas de negocio dentro de la organización. Los cuales deben tener una comprensión completa de sus propias funciones, además de una percepción global de la organización.

2.2.3 Reunión Inicial del Proyecto

En esta reunión se debe establecer los objetivos del proyecto y sus documentos entregables, estos deben ser claramente definidos, es necesario puntualizar que todos los esfuerzos deben estar fijados en conseguir los objetivos del BCP.

Los objetivos y documentos entregables deben ser aprobados por la gerencia de la organización.

Adicionalmente se deben proponer sub-objetivos para cubrir las tareas de desarrollo o inclusive para realizar capacitaciones sobre el desarrollo del BCP y de esta forma garantizar que los empleados entienden sus responsabilidades en la ejecución del plan.

Adicionalmente debe tomarse en cuenta las políticas de seguridad y planes de contingencia son rentables.

Los entregables a considerar son:

- Análisis del riesgo e impacto en el negocio.
- Procedimientos de recuperación.
- Plan de recuperación de desastres.
- Plan de Pruebas
- Plan de entrenamientos
- Procedimientos para mantener el plan actualizado.

2.2.4 Puntos de Revisión

Es importante establecer puntos control en el proyecto con la finalidad de realizar seguimiento del progreso del cronograma.

Los puntos a revisar son:

- Aprobación del proyecto
- Reunión inicial
- Plan de análisis de riesgos e impacto en el negocio.
- Plan de emergencias
- Plan de pruebas de BCP
- Plan de entrenamiento
- Aprobación de BCP
- Actividades de Plan de pruebas
- Actividades de Plan de entrenamiento.

2.3 FASE 1: DESARROLLO DEL PLAN DE TRABAJO

Se plantea el desarrollo del trabajo, detalle de los objetivos y alcance del proyecto, se definen las actividades y responsables con recursos y duración de las mismas.

Se estudian los limitantes y riesgos, así como dependencias de otras áreas, para terminar con estrategias de comunicación y seguimiento del proyecto.

Se realizará la política de BCP, identificando normas regulatorias y objetivos estratégicos. Una vez finalizada la política se realizan revisiones y aprobación por parte de la Dirección. Se debe establecer el comité del BCP con coordinación y áreas de soporte.

En este primer paso se identifican los requerimientos del negocio y de los clientes, así como las dependencias externas tales como leyes del gobierno e industriales.

Es importante obtener el apoyo de la gerencia en este punto del desarrollo del BCP.

2.4 FASE 2: ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)

Desarrollo del análisis del impacto al negocio identificando, cuantificando y calificando el impacto al negocio por pérdida o interrupción de las operaciones, proveer la información con la que se determinen estrategias de recuperación apropiadas.

2.4.1 Actividades Principales

Las actividades que comprende esta fase son:

- Definición, ponderación y aprobación de los niveles de impactos cualitativos y cuantitativos a utilizar.

- Desarrollo de procedimiento de análisis del impacto al negocio.

- Programación de entrevistas, talleres y aplicación de cuestionarios con los responsables de las operaciones de acuerdo al procedimiento definido.

- Identificar tiempo máximo de tolerancia a no disponibilidad de los sistemas y recursos (MTO)[2]

- Establecer objetivos de punto de recuperación (RPO)[3]

- Establecer objetivos de tiempo de recuperación (RTO)[4]

- Reconocimiento de períodos críticos de operación.

- Revisión y aprobación de los resultados del BIA

2.5 FASE 3: ESTRATEGIAS DE RECUPERACIÓN

Se desarrollan estrategias para garantizar que los procesos de negocio puedan restablecerse dentro de los plazos requeridos RTO. Se incluyen controles destinados a identificar y reducir riesgos, atenuar consecuencias de los incidentes y asegurar la reanudación oportuna de las operaciones indispensables.

Se identifican y evalúan los riesgos relacionados a la continuidad de las operaciones; es decir la probabilidad y el impacto de una variedad de amenazas que pudieran ocasionar interrupciones a dichos servicios.

[2] Maximun Tolerable Outage
[3] Recovery Point Objective
[4] Recovery Time Objectiv

Posteriormente se priorizan los riesgos y se determinan medidas a implementar para mitigarlos.

2.5.1 Actividades Principales

Las actividades que comprende esta fase son:

- Revisión del alcance, las premisas y los hallazgos del BIA.
- Generación de diversas opciones de estrategias a seguir, para su discusión y análisis, considerando análisis costo-beneficio.
- Revisión, selección y aprobación de las estrategias por parte de la Dirección.
- Definición de proyectos y responsables para el desarrollo de planes de recuperación de las operaciones alineados a las estrategias.
- Definición de un sistema de calificación de impactos y probabilidades para calcular el riesgo.
- Identificación de las amenazas a la continuidad de las operaciones.
- Determinación del nivel de impacto y la probabilidad de ocurrencia de las amenazas.
- Cálculo del riesgo con base en el impacto y probabilidad de las amenazas. Establecimiento de prioridades y determinación de las medidas adecuadas para el tratamiento de cada riesgo identificado, considerando las alternativas para reducirlo, transferirlo, evitarlo o aceptarlo.

2.6 FASE 4: IMPLEMENTACIÓN DEL PLAN

Se desarrollan planes con los procedimientos a seguir para la recuperación de las operaciones críticas posterior a un evento de desastre que interrumpa la continuidad del negocio. Los planes a desarrollar deben soportar las estrategias de recuperación seleccionadas. Se contempla el desarrollo de restauración es decir el regreso a la operación una vez restablecidos el sitio y los recursos de operación primarios.

2.6.1 Actividades Principales

Las actividades que comprende esta fase son:

- Nombrar a los responsables de elaborar y revisar las actividades específicas de recuperación.
- Definición de la estructura, formato, componentes y contenido de los planes.
- Determinar la logística para la documentación de planes.
- Obtener la información necesaria para contenido de los planes.
- Elaboración de planes documentados.
- Circular los planes para su revisión.
- Adecuación de los planes y obtener aprobaciones.
- Asesoría en el desarrollo de esquemas de operación alternativos por parte de los responsables.

2.7 FASE 5: PROGRAMA DE SOPORTE

El plan de continuidad de negocio debe mantenerse mediante revisiones y actualizaciones periódicas para garantizar su eficacia permanente ante cambios. Una buena práctica es realizar actualizaciones anuales.

2.7.1 Entrenamiento

Definición y ejecución de un programa de concientización y entrenamiento dirigido al personal involucrado en la recuperación y restauración de las operaciones.

2.7.2 Actividades Principales

Las actividades que comprende esta fase son:

- Definición de los conocimientos y mensajes específicos que deben ser asimilados por el personal involucrado.

- Definición de la audiencia y la logística para el entrenamiento.

- Ejecución del entrenamiento con fines de capacitación y concientización.

Entre los puntos a considerar en el temario de entrenamiento inicial están:

- Estrategias del BCP/DRP.
- Organización del BCP/DRP.
- Estructura y contenido de los planes.
- Responsabilidades.
- Apoyo para mantenimiento y pruebas de los planes.

2.7.3 Pruebas y Ejercicios

Desarrollar el plan de pruebas y ejercicios de los planes de recuperación considerando los diferentes tipos:

- Pruebas de escritorio
- Pruebas simuladas
- Pruebas en producción (parciales o completas)

Los principales puntos a considerar en la conducción de las pruebas o ejercicios serán:

- Definición y acuerdo del alcance y los objetivos.
- Estimación y aprobación de presupuesto.
- Definición y asignación del personal participante.
- Definición de los escenarios y supuestos.
- Evaluación de posibles impactos a las operaciones en producción.
- Conducción de la prueba o ejercicio.
- Registro y reporte de los resultados.
- Generación de planes de corrección de hallazgo.

2.7.4 Mantenimiento

Figura 2.1: Planes del BCP

Fuente: La Autora

Se desarrolla el plan de mantenimiento del BCP para asegurar que las áreas permanezcan preparadas para el manejo de incidentes relacionados a la continuidad del negocio a pesar de los cambios de personas, procesos y tecnología.

Los siguientes son indicadores del mantenimiento del plan:

- Revisión periódica del BCP (mantenimiento programado).
- Control de cambios y adecuaciones al plan.
- Pruebas y/o ejercicios y adecuaciones al plan.

2.8 METODOLOGÍA

2.8.1 Sistema de Gestión de Seguridad de Información

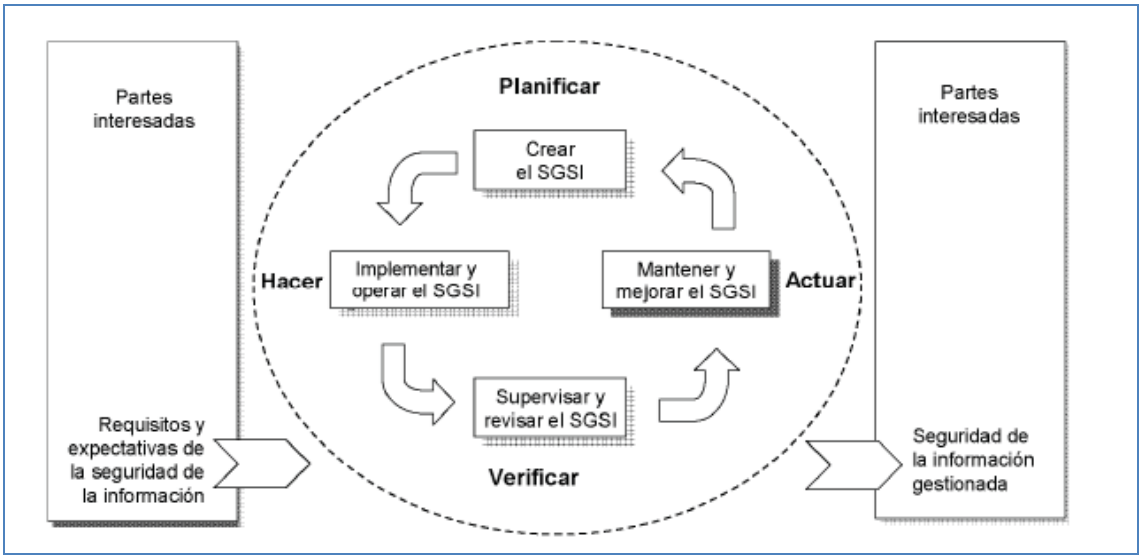
Como parte primordial del Plan de Continuidad de negocios es necesario desarrollar el SGSI (Sistema de gestión de seguridad e información) que

certifica que los riesgos de la seguridad de la información sean conocidos, aceptados, gestionados y minimizados por la organización de forma eficaz, documentada, ordenada, metódica, cíclica y maleable a cambios.

El análisis de riesgos es un procedimiento de ayuda en la decisión sobre nuevos mecanismos de seguridad, sus resultados constituyen una guía para la organización sobre los controles y procesos de seguridad más adecuados.

Sin embargo el nivel del riesgo de una entidad no podrá erradicarse por completo, el objetivo es buscar un equilibrio entre los recursos y mecanismos que se deben dedicar para reducir riesgos y llegar a un nivel de seguridad aceptable.

Figura 2.2: Método PDCA



Fuente: ISO/IEC 17799

La metodología está basada en el estándar BS 25999-1 que presenta los procesos y principios necesarios para una adecuada gestión de la continuidad del negocio que permita cubrir las necesidades de clientes y organizaciones, basado en un Sistema de Gestión de Riesgos.[5]

[5] ISO/IEC 17799 Versión Española

Esta norma internacional sigue el modelo “Planificar-hacer-verificar-actuar” (Plan-Do-Check-Act conocido como modelo PDCA[6]) que se aplica para estruturar todos los procesos del sistema de gestión de riesgos.

2.8.2 Conceptos en el Análisis y Gestión de Riesgos

El análisis de riesgo es la consideración del daño probable que puede causar un fallo en la seguridad de la información tomando en cuenta pérdida de autenticidad, confidencialidad, integridad y disponibilidad de la misma.

Los factores a determinarse deben ser evaluados de forma imparcial y objetiva ya que al realizar un análisis erróneo la garantía que ofrece el análisis de riesgo no cumplirá su función principal de proteger los activos.

“La medición de riesgos es el primer paso de control y la mejora. Si algo no se puede medir, no se puede entender. Si no se entiende, no se puede controlar. Si no se puede controlar no se puede mejorar”.[7]

El análisis de riesgos parte de la definición de activos y amenazas, por lo que es necesario conocer los siguientes conceptos:

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.

[6] PDCA - Círculo de Deming o circulo de Gab ESTRATEGIA DE MEJORA CONTINUA DE CALIDAD

[7] H. James Harrington

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 la organización.

Confidencialidad

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

La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Autenticidad

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 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 es 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:

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.

Activo

Es un recurso físico o lógico que constituyen infraestructura, patrimonio, conocimiento y reputación de una entidad.

Amenaza

Es un evento o incidente provocado por un ente hostil a la empresa, valiéndose de las vulnerabilidades de un activo con el fin de agredir la confidencialidad, integridad o disponibilidad del mismo. Las amenazas pueden ser internas o externas, así también pueden ser deliberadas o accidentales. Entre las amenazas posibles están: errores, ataque o daño intencional, fraude, robo, falla de software o hardware, desastres naturales.

Vulnerabilidades

Existe un factor adicional que es la vulnerabilidad y es la circunstancia o característica que permite la consecución de ataques que comprometan la integridad, confidencialidad y disponibilidad del activo.

Impacto

Magnitud de las consecuencias que tiene el negocio al poseer activos que puedan comprometer su disponibilidad en todos sus aspectos, esto es debido a que una o varias amenazas hayan explotado sus vulnerabilidades.

Salvaguardas

Políticas, procedimientos, normas, procesos o mecanismos son considerados salvaguardas o en su defecto todo control que posea una entidad. Esto contribuye a reducir las vulnerabilidades, reducir probabilidad de que las amenazas se efectivicen, reducir el impacto producido por la materialización de amenazas.

Estos se miden por el costo de adquisición y la dificultad de implementación.

Tipos de salvaguardas

Preventivas

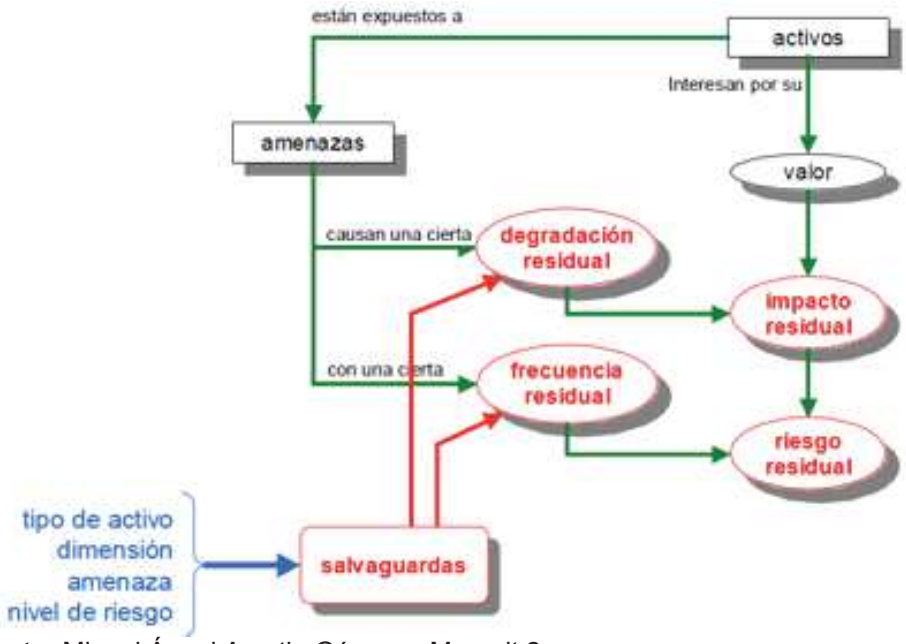
Estas contribuyen a prevenir que se materialicen los riesgos, protegen a los activos antes de que sufran ataques, reduciendo de esta forma la frecuencia de amenazas. Estos son políticas de seguridad, formación de usuario, controles de acceso, segregación de funciones, entre otras.

Reactivas

Estas detectan la amenaza ya sea en el instante del inicio de su ejecución o permitiendo que inicien sin avanzar, de esta forma la amenaza se materializa pero es neutralizada por el salvaguarda, limitando así el daño causado, en ocasiones la amenaza logra su objetivo pero el salvaguarda logra la

restauración, se encuentran registros de logs, sistema de detección de intrusos, sistema de respaldos, plan de contingencias, etc.

Figura 2.3: Ciclo Salvaguardas



Fuente: Miguel Ángel Amutio Gómez – Magerit 2

2.8.3 Desarrollo del Análisis y Gestión de Riesgos

Es necesario detallar el objetivo y conclusiones que se conseguirán con el análisis y gestión de riesgo.

Como se ha establecido con anterioridad, el análisis de riesgos busca determinar tiene los activos de la Organización y avizorar sucesos posteriores, los elementos a tomar en cuenta serán los activos, amenazas y salvaguardas.

Se podrá estimar el impacto y riesgo, esto por medio de un análisis metódico

2.8.4 Análisis de Riesgo

Se determina el riesgo a través de las siguientes actividades:

Establecer los activos relevantes para la organización, así como su valor e interrelación, consiguiendo así el costo o pérdida que supondría su pérdida.

Establecer las amenazas a las que están expuestos los activos.

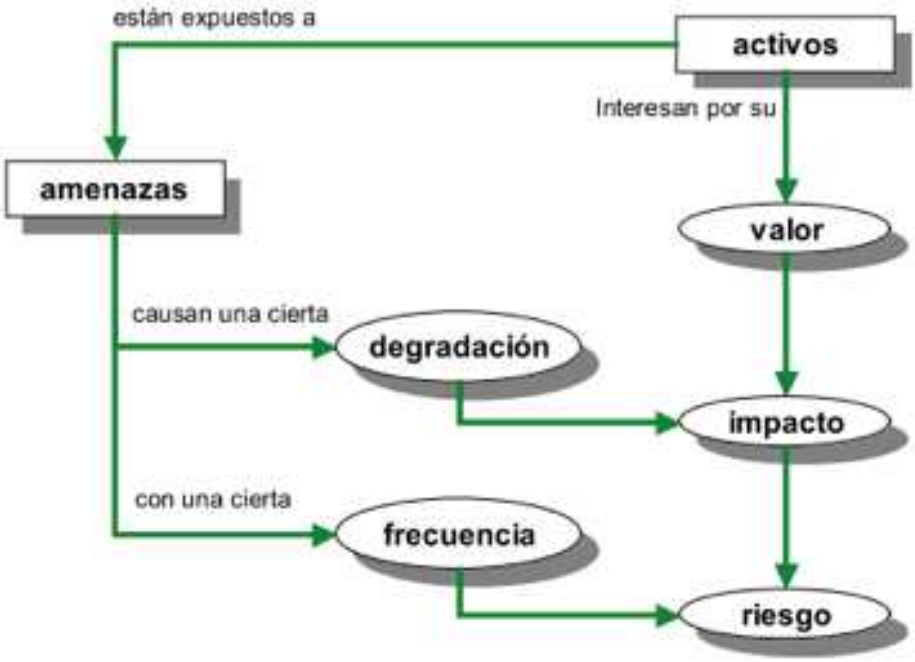
Establecer que salvaguardas estarían disponibles y cuales serías las mas adecuadas para dichos activos.

Evaluar el impacto que tendría el activo de acuerdo a las amenazas establecidas.

Estimar la probabilidad de ocurrencia de las amenazas.

Con el objetivo de establecer los riesgos y con miras a definir una pérdida completa o riesgos potenciales se realiza un estudio sin tomar en cuenta las salvaguardas, esto como un escenario teórico, una vez definido este primer escenario se realiza el estudio y la incorporación de salvaguardas al plan.

Figura 2.4: Escenario Teórico de Análisis de riesgo



Fuente: Miguel Ángel Amutio Gómez – Magerit 2

2.8.5 Activos

La información principal a encontrar es la información o datos que maneja el sistema, y partiendo de estos se puede considerar otros activos relevantes.

2.8.5.1 Tipos de Activos

Es necesario clasificar los activos por su tipo ya que las amenazas y las salvaguardas son diferentes según su tipo.

Esta clasificación no puede considerarse definitiva, debido a que existen cambios constantes, por tal motivo el primer estudio o clasificación se toma como referencia.

Los activos deben clasificarse de acuerdo a una jerarquía, un activo conforme a sus características o usos puede pertenecer a varios tipos de activos.

Servicios que pueden incluirse en base a datos, o servicios que puedan necesitarse para tramitarlos.

Los servicios satisfacen la necesidad de un usuario, un cliente. Estos pueden ser servicios finales, servicios instrumentales, es decir que los medios y usuarios pertenecen a la empresa; servicios contratados, servicios públicos, servicios empresariales, servicios internos, etc.

Al realizar un análisis de riegos de la tecnología de la información y comunicaciones surgen los servicios de información, servicios de comunicaciones, servicios de seguridad, etc.

Datos que son elementos de la información que representan conocimiento e información.

Estos son los que permiten a una entidad brindar servicios, son activos almacenados por lo general se encuentran como base de datos. En un análisis de riesgos este activo es primero en la cadena de valoración dejando así como secundarios al resto de activos sin embargo no de menor importancia.

Entre los tipos de datos encontramos datos vitales, datos de interés comercial, datos de gestión interna, multimedia, código fuente, código ejecutable, datos de configuración, datos clasificados, datos personales etc.

Software que permite manejar los datos. Estos programas gestionan, analizan, y transforman los datos permitiendo así transformar la información para prestación de servicios.

Encontramos tipos de programas tales como; de desarrollo propio, desarrollo a medida, desarrollo estándar, navegador web, antivirus, sistema operativo, servidor de terminales, sistema de backup.

Hardware o equipo informativo; estos son bienes físicos que están destinados para alojar temporal o definitivamente datos, estos soportan directa o indirectamente los servicios, también pueden ser equipos responsables de transmitir datos.

Los tipos de hardware a citar son: grandes equipos tales como servidores; estos necesitan un entorno específico para su desempeño, no se encuentran en gran cantidad. Los que se encuentran en mayor cantidad, costo medio y de reemplazo medio son los llamados equipos medios. Los equipos de Informática personal tiene un costo pequeño con un requerimiento de entorno mínimo de operación y de fácil reemplazo. Los de fácil transporte están dentro de Informática móvil. Equipos para transmisión de datos tales como routers, modems etc.; equipos de almacenamiento estos son los que almacenan información por un largo plazo no así con los que solo manejan información en tránsito. Así también existen agendas electrónicas, periféricos, central telefónica, medios de impresión entre otros.

Redes de comunicaciones son los medios para transportar información entre los principales encontramos; RDSI, X25, ADSL, P2P, Wirelless, satelital, LAN, WAN, Internet, VPN etc.

Soportes de información; son dispositivos físicos que permiten almacenar información de forma permanente entre otros están: discos duros, cd's, USB, DVD, cintas magnéticas, tarjetas de memoria, material impreso, microfilms etc.

Equipamiento auxiliar; se consideran a los equipos que sirven de soporte sin estar relacionados directamente con los datos como: fuentes de alimentación, UPS, Generadores eléctricos, equipos de climatización, cableado, robots, mobiliario, cajas fuerte etc.

Instalaciones que hospedan equipos informáticos tales como edificios, locales, vehículos, contenedores, etc.

Personal: Estos son los administradores y usuarios de equipos mencionados anteriormente como usuarios internos y externos, operadores, administradores de sistemas, administradores de comunicaciones, administradores de Bases de datos, desarrolladores, proveedores etc.

Dependencias

Existen equipos superiores o de mayor importancia que depende de activos de menor rango o importancia, por tal razón es importante realizar un estudio de las dependencias entre activos.

Es posible encontrar que al verse efectiva una amenaza sobre un equipo inferior, este afecte directamente el desempeño del activo superior.

En cada organización debe realizarse un análisis para identificar la estructura de activos, pero es mas frecuente realizar una estructura en capas donde las capas superiores dependen de las inferiores:

Capa 1: el entorno; activos necesarios para avalar las faltantes capas: Equipos y suministros, Edificios, Personal.

Capa 2: Sistemas de información: tales como equipos informáticos, aplicaciones, comunicaciones, soportes de información.

Capa 3: Información: datos, meta-datos.

Capa 4: Funciones de la organización: estos dan una funcionalidad y sentido a la existencia del sistema.

Capa 5: Otros activos tales como conocimiento, credibilidad, integridad física del personal etc.

2.8.6 Valoración

Es necesario determinar los activos que tienen valor para la entidad con el objetivo de proteger, por esta razón es imprescindible analizar y evaluar los activos para su valoración. Este valor puede ser unitario o acumulado.

La vulnerabilidad de un activo se mide en dos sentidos tales como su degradación es decir cuan afectado resultaría el activo y en su frecuencia o cada cuanto se presenta la amenaza.

La frecuencia coloca en perspectiva a la degradación, de acuerdo a su probabilidad de materialización y sus consecuencias.

La frecuencia puede verse explicada a continuación:

100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años

2.8.7 Dimensiones de Valoración

Estos son atributos que dan valor a un activo, es posible realizar análisis de atributos basándose en un único atributo del activo sin tomar en cuenta otros. Las dimensiones son útiles para asignar un valor al activo en caso de ser víctima de una amenaza efectiva, también dan señales de la magnitud del daño que provocaría a la empresa.

Estas son:

1 Disponibilidad: Esta es una característica que afecta a todo tipo de activos, es la certeza de que el usuario tiene acceso a la información autorizada cuando lo requiera.

2 Integridad de datos: Información completa y exacta así como los métodos de sus procesos.

3 Confidencialidad de datos: Garantía de que la información tiene restricción y acceso a las personas correctas.

4 Autenticidad de los usuarios del servicio: Garantía de la identidad y origen del usuario, esto asegura que el mal uso o uso no autorizado sea efectivo.

5 Autenticidad del origen de datos: Garantiza la identidad y origen de la fuente, es decir los datos son imputables a quien deben.

6 Trazabilidad del servicio: Garantía para determinar quien hizo, que y en qué momento. Asegurando constancia o log del uso de servicios.

7 Trazabilidad de los datos: Asegura constancia de log de acceso a datos.

2.8.8 Criterios de Valoración

Para realizar la valoración es importante que se utilice una escala común para todas las dimensiones y de esta forma comparar riesgos, utilizar una escala basada en diferencias de valor y un criterio paralelo que permita comparar análisis realizados indistintamente.

Para la valoración debe tomarse en cuenta como punto de referencia:

- Seguridad del personal
- Obligación de ley
- Intereses comerciales y económicos
- Pérdidas financieras
- Interrupción del servicio
- Orden público
- Política corporativa
- Otros valores intangibles

La valoración puede ser cualitativa o cuantitativa en donde los criterios mas importantes son la Homogeneidad y la relatividad.

Valoración cualitativa: Usa escala de niveles, posicionando al activo en orden relativo respecto a los demás.

Valoración cuantitativa: Son valoraciones numéricas absolutas, por lo que la interpretación de los resultados no dan lugar a controversias.

Valoración del servicio: La disponibilidad es una dimensión que no es posible medir igual que las otras dimensiones debido a que las consecuencias varían de acuerdo a su tiempo de interrupción, en este caso la disponibilidad no recibe un solo valor sino tantos como escenarios se disponga.

2.8.9 Amenazas

Establecer las amenazas que afecten a los activos. Tales como accidentes naturales, desastres industriales, el objetivo es establecer o identificar la lista de amenazas, fuentes que son aplicables al sistema informático que se está evaluando.

2.8.9.1 Tipos de Amenazas

1 Desastres naturales: son los que pueden ocurrir sin la intervención del ser humano, tales como fuego, daños por agua, terremotos, rayos, etc.

2 Desastres de origen industrial: estos pueden ocurrir en forma accidental o deliberada provenientes de la actividad humana en el medio industrial, en estos están incluidos daños por fuego, agua, explosiones, derrumbes, sobrecarga de electricidad, etc.

3 Errores y fallos no intencionados son los que son causados no intencionalmente por las personas, tales como errores de configuración, errores de monitoreo, errores de usuario, degradación de la información, divulgación de la información, etc.

4 Ataques intencionados son fallos causados por personas deliberadamente, son similares a los errores no intencionados pero difieren en la intención o propósito, así como manipulación de la información, suplantación de identidad, robo de equipos, etc.

2.8.10 Correlación de Errores y Ataques

Debe conocerse la diferencia entre errores y ataques debido a que existe correlación entre ambas, ya que pueden existir:

- Amenazas que se presentan siempre por errores
- Amenazas que siempre son ataques
- Amenazas que pueden ser ataques o errores.

2.8.11 Amenazas por Tipo de Activo

Las amenazas pueden presentarse por tipo de activo, indicando en que aspecto se verán afectados en mayor escala.

Así los servicios y datos se verán afectados con la amenazas de errores y fallos no intencionados y con ataques intencionados.

Las aplicaciones están expuestas a las mismas amenazas que los servicios y datos, se verán afectadas por una amenaza de Origen Industrial.

Las amenazas tales como desastres naturales, de origen industrial, los errores y fallos no intencionados y los ataques intenciones afectarán los activos como equipos informáticos o hardware.

Las redes de comunicaciones se verán afectadas por todas las amenazas en mayor escala.

Los soportes de información pueden sufrir amenazas tales como desastres naturales y de origen industrial en sus áreas de trazabilidad y disponibilidad.

A continuación la siguiente tabla de la relación entre posibles errores y ataques:

Tabla 2.1: Relación error-ataque

N°	Error	Ataque
1	Errores de los usuarios	
2	Errores del administrador	
3	Errores de monitorización (log)	
4	Errores de configuración	Manipulación de la configuración
5	Suplantación de la identidad del usuario	
6		Abuso de privilegios de acceso
7	Deficiencias en la organización	Uso no previsto
8	Difusión de software dañino	Difusión de software dañino
9	Errores de [re-]encaminamiento	[Re-]encaminamiento de mensajes
10	Errores de secuencia	Alteración de secuencia
11		Acceso no autorizado
12		Análisis de tráfico
13		Repudio
14	Escapes de información	Interceptación de información
15	Alteración de la información	Modificación de la información
16	Incorrecta. Introducción de falsa información	Introducción de información
17	Degradación de la información	Corrupción de la información
18	Destrucción de información	Destrucción la información
19	Divulgación de información	Divulgación de información
20	Vulnerabilidades de los programas	
	(software)	
21	Errores de mantenimiento/actualización de programas (software)	
22		Manipulación de programas
23	Errores de mantenimiento / actualización de equipos (hardware)	
24	Caída del sistema por agotamiento de recursos	Denegación de servicio
25		Robo
26		Ataque destructivo
27		Ocupación enemiga
28	Indisponibilidad del personal	Indisponibilidad del personal
29		Extorsión
30		Ingeniería social

Fuente: Metodología Magerit Tomo I

Son mayores las amenazas en el área de disponibilidad y trazabilidad en el tipo de activos de equipamiento auxiliar, siendo de menor número las amenazas en integridad y confiabilidad.

Las instalaciones pueden sufrir las mismas amenazas de desastres naturales y de origen industrial en las áreas de trazabilidad y disponibilidad, presentando la misma amenaza de ataques intencionados con respecto a confiabilidad, integridad y autenticidad.

El personal está expuesto a las amenazas de errores y fallos no intencionados así como ataques intencionados en todas sus dimensiones.

Como se ha detallado con anterioridad, las amenazas para la disponibilidad son diferentes y se miden de forma independiente, el siguiente cuadro detalla las amenazas de acuerdo a sus áreas y tipos de activos.

Tabla 2.2: Impacto de Amenazas

TIPO DE ACTIVOS	DESTRUCCIÓN	AVERÍA		SATURACIÓN	CARENCIA
		FÍSICA	LÓGICA		
SERVICIOS			EYF – AI	EYF – AI	
DATOS	EYF – AI				
SOFTWARE			EYF – AI – OI	AI	
HARDWARE	DN – OI – AI	DN – OI	OI – EYF	AI – EYF	OI – AI
COMUNICACIONES	DN – OI – AI	DN – OI	OI – EYF	AI – EYF	OI – AI
SOPORTES DE INFORMACIÓN	DN – OI – AI	DN- OI		AI	OI – AI
EQUIPAMIENTO AUXILIAR	DN – OI – AI	DN- OI		AI	OI – AI
INSTALACIONES	DN – OI – AI	DN- OI		AI	
PERSONAL			EYF		EYF –AI

EYF:	ERRORES Y FALLOS NO INTENCIONALES
AI:	ATAQUES INTENCIONADOS
OI:	ORIGEN INDUSTRIAL
DN:	DESASTRES NATURALES

Fuente: Metodología Magerit Tomo I

Es propio analizar el impacto de las amenazas que se materializarán en los activos y generarán posibles daños.

Impacto Acumulado: Es el valor del activo tomando en cuenta el valor del mismo, sus dependencias y las amenazas a las que está expuesto.

Este impacto es calculado de acuerdo a cada valor del activo y su amenaza y en cada dimensión. Así el impacto se incrementará mientras el valor del activo y sus dependencias crezcan.

Este tipo de impacto permite establecer salvaguardas para los medios de trabajo que son los que soportan el peso del sistema de información.

Es necesario tomar en cuenta que este riesgo solo puede ser agregado cuando:

- Los activos no son dependientes entre si
- Los activos no dependen de un activo superior común
- Los activos deben ser independientes

Impacto Repercutido: las variables que se toman en cuenta en este cálculo son el valor propio del activo y las amenazas de los activos de los que depende, así también el cálculo es en base a cada amenaza por cada dimensión.

El impacto va de acuerdo al valor del activo, así como la degradación o daño, y mientras más dependencias tenga.

Es posible establecer las consecuencias en las ocurrencias técnicas y de esta forma establecer un cierto nivel de riesgo aceptable.

Para ambos tipos de impacto es necesario tomar en cuenta que los riesgos solo pueden ser agregados cuando:

- Los activos no son dependientes entre si.
- Los activos no dependen de un activo superior común.
- Los activos deben ser independientes
- Las amenazas se presentan en diferentes dimensiones.

2.8.12 Determinación del Riesgo

El riesgo es el probable daño cuantificable sobre un sistema. El riesgo se puede decretar con la determinación del impacto que tienen las amenazas sobre los activos. La frecuencia de ocurrencia es el punto a tomar en cuenta para determinar el riesgo.

Al igual que el impacto tenemos dos tipos de riesgo, estos crecen con el impacto y la frecuencia.

Riesgo Acumulado: tomar en cuenta el impacto acumulado, la frecuencia de la amenaza y el efecto directo de las amenazas sobre el activo. Este riesgo supone el valor del daño de la organización.

Riesgo Repercutido: para determinar el riesgo repercutido debe tomarse en cuenta el impacto repercutido debido a una amenaza sobre un activo y la frecuencia de la amenaza.

Se deben tomar en cuenta las mismas precauciones de los impactos para la agregación de riesgos a los activos.

2.8.13 Salvaguardas

Definido como procedimiento o recursos electrónicos que reducen los riesgos. Existen amenazas que son neutralizadas simplemente ejecutando políticas o estableciendo seguridades físicas.

Existen diferentes aspectos en los cuales una salvaguarda puede ejercer su capacidad para limitar impacto y mitigar el riesgo.

- Procedimientos
- Política de personal
- Soluciones técnicas
- Software
- Hardware
- Protección a las telecomunicaciones
- Física

La salvaguarda idónea es teóricamente eficiente, completamente desplegada, configurada y mantenida; se emplea siempre, contiene procedimientos claros de uso normal y para incidentes, posee usuarios capacitados y controles con alarmas en caso de fallos.

Debe tomarse en cuenta que un salvaguarda debe estar equilibrado en diferentes aspectos, debe estar adecuada a cada tipo de activo y cada tipo de dimensión.

2.8.14 Impacto y Riesgo Residual

La determinación del impacto realizado en primera instancia es el que no toma en cuenta las salvaguardas, es decir se realiza el análisis de impacto tomando en cuenta el peor escenario sin ningún tipo de preventiva.

En este caso debe realizarse el análisis verificando las salvaguardas para llegar a un impacto razonable.

Impacto Residual: Si se ha realizado un análisis completo y en forma correcta, el impacto residual sería algo bajo, en el caso de haber realizado un análisis impreciso entonces el sistema permanecerá bajo un impacto residual constante.

El impacto y el riesgo residual se calculan de la misma forma que el impacto o riesgo normal, agregando este nuevo nivel de degradación.

2.8.15 Implementación y Operación del Sistema de Gestión de Riesgos

Luego de realizar el análisis y conocer los riesgos se los debe gestionar y aceptar el riesgo, mitigar el riesgo por medio de los salvaguardas analizadas por su costo y beneficio.

Definir el modo de medir eficacia de los controles o de los grupos de controles seleccionados y especificar como tienen que usarse estas mediciones para evaluar la eficacia de los controles de cara a producir unos resultados comparables y producibles.

Implementar procedimientos y otros controles que permitan una detección temprana de eventos de seguridad y una respuesta ante cualquier incidente.

El objetivo de la gestión de riesgos es equilibrar los costos de controles y su efectividad al reducir los riesgos.

La gestión de riesgos es el conjunto del análisis de riesgos mas el tratamiento de los mismos.

Este debería proporcionar un informe de fácil manejo para la dirección de la entidad, emitiendo detalle de activos o riesgos a eliminarse inmediatamente obteniendo así reducción eficaz y sin costo de riesgos.

Según la ISO 27001 “Hay que desarrollar criterio para la aceptación del riesgo e identificar el nivel de riesgo aceptable”

Para el tratamiento de los riesgos es necesario aceptarlos, transferirlos y mitigarlos.

2.8.16 Supervisión y Revisión

Se ejecutan procedimientos de supervisión y revisión, así como otros mecanismos de control para:

- Detectar lo antes posible los errores en los resultados del proceso.
- Identificar lo antes posible las debilidades del sistema de seguridad.
- Permitir a la dirección determinar si las actividades de seguridad dan resultados esperados.
- Ayudar a detectar eventos de seguridad y prevenir incidentes mediante indicadores.

Realizar revisiones periódicas de eficacia, tendiendo en cuenta resultados de mediciones, sugerencias y comentarios de todas las partes interesadas.

Revisar los cambios en la organización, tecnología, objetivos empresariales, amenazas, factores externos, etc.

Realizar revisiones o auditorías internas.

2.8.17 Mantenimiento y Mejoras

Implementar mejoras identificadas, aplicando medidas correctivas y preventivas adecuadas, comunicar las mejoras a todas las partes interesadas con un nivel de detalle de acuerdo al tipo de actualización. Asegurar que las mejoras alcancen los objetivos previstos.

2.8.18 Concienciación, Formación y Capacitación

La organización debe asegurar que todo el personal al que se le hayan asignado responsabilidades definidas sea competente para llevar a cabo tareas requeridas a través de:

- Determinar las competencias necesarias para el personal que lleva a cabo trabajos que afecten el sistema de seguridad.

- Impartir formación o realizar otras acciones por ejemplo la contratación de personal competente para satisfacer estas necesidades.

- Evaluar la eficacia de las acciones realizadas.

- Mantener registros de evaluación, formación, aptitudes, experiencias y cualificaciones.

2.8.19 Requisitos de la Documentación

La documentación debe incluir decisiones de la Dirección junto con los registros de las mismas, debiendo quedar constancia de que las acciones dan respuesta a las decisiones y políticas adoptadas y garantizando que dichos documentos y registros están disponibles.

La documentación debe demostrar la relación de los controles seleccionados con los procesos de evaluación y de tratamiento de riesgos.

Control de documentos

La documentación debe incluir alcance, procedimientos o mecanismos de control, informe de evaluación de riesgos, plan de tratamiento de riesgos, procedimientos documentados para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información.

Los documentos exigidos deben estar protegidos y controlados, se debe revisar, actualizar y volver a aprobar los documentos según vaya siendo necesario, asegurar que están identificados los cambios y el estado del documento que tiene la última versión, se debe verificar que los documentos estén disponibles, asegurar que los documentos sean debidamente distribuidos.

Control de registros

Se debe crear y mantener registros para proporcionar evidencias de la conformidad con los requisitos y del funcionamiento eficaz. Dichos registros deben estar en cuenta cualquier requisito legal o regulatorio aplicable, así como las obligaciones contractuales. Los registros deben permanecer legibles fácilmente identificables y recuperables. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, retención y disposición de los registros deben estar documentados e implementados.

Deben conservarse los registros del desarrollo del proceso y de todos los sucesos derivados de incidentes de seguridad significativos relativos al proceso de seguridad.

2.8.20 Compromiso de la Dirección

La Dirección debe suministrar evidencias de su compromiso para todos los pasos del proceso velando por el establecimiento de los objetivos y planes, estableciendo los roles y responsabilidades en materia de seguridad de información, comunicando a la organización la importancia de cumplir con los objetivos del plan, decidiendo los criterios de aplicación de riesgo y los niveles aceptables, dirigiendo revisiones y velando que se realicen los controles internos o auditorías.

CAPITULO III

3 DESARROLLO BCP

3.1 SITUACIÓN ACTUAL

Para realizar el plan de continuidad de negocios es necesario efectuar un análisis del estado actual de la empresa para lo cual se ejecutarán revisiones de control.

Se cubrirán los siguientes puntos de revisión:

- Administración de riesgos:
- Seguridad de cuarto de servidores
- Administración de seguridad
- Procesos de entrada y salida de usuarios
- Acuerdos de confidencialidad
- Protección de información
- Administración de Activos
- Administración de equipos Hardware
- Software
- Protección de virus
- Servicios de soporte
- Administración de Help Desk
- Administración de cambios
- Administración de base de datos
- Administración de base de datos SQL
- Administración de base de datos DB2
- Otras bases de datos
- Sistemas operativos en red

- UNIX/LINUX
- Windows
- Sistema distribuido AS400
- Servicios e infraestructura de red LAN
- Sistemas de correo electrónico
- Call Center
- Seguridad de dispositivos móviles
- Operaciones de diseño, ingeniería y fábrica
- Sistemas de Diseño
- Maquinas de fábrica
- Revisión de aplicaciones

3.2 ANÁLISIS DEL PROBLEMA

Se realizó la revisión de los sistemas de información, la conformidad con las prácticas profesionales es el enfoque que se ha tomado en cuenta para la revisión y evaluación de la seguridad y la administración del entorno informático de la unidad.

Se ha comparado la administración actual de los procedimientos de seguridad con las costumbres generalmente aceptadas.

Como conclusión, el sistema de seguridad que actual y la administración de los sistemas de información no son satisfactorios.

Informe de seguridad y entorno informático

En el siguiente cuadro se detalla los puntos de revisión y el informe del estado actual de seguridad de la empresa.

Tabla 3.1: Puntuación informe seguridad IT

Puntaje de Revisión	*55 puntos*
Insatisfactoria	
Índice de Revisión	**Puntos**
Ambiente de Control Correcto	0-20
Necesita mejoras	21-39
Insatisfactoria	40 +

Fuente: La Autora

Tabla 3.2: Detalle de puntuación por puntos de revisión

Puntos de revisión:	*Riesgo*
Respaldo de información	Amarillo
Protección de información	Amarillo
Administración de cuentas	Amarillo
Administración de Hardware	Amarillo
Seguridad de red inalámbrica	Amarillo
Seguridad Cuarto de servidores	Amarillo
Administración y políticas de Servidores	Amarillo
Administración de software: Licencias, Open Source, Software Ilegal	Amarillo
Revisión de aplicaciones	Amarillo
Computer Disaster Recover Plan (cDRP)	Amarillo
Administración de seguridad	Amarillo
Encriptación de datos	Verde
Administración de cambios	Verde
Acuerdos de propiedad de información	Verde
Seguridad de dispositivos móviles	Verde
Documentación de procesos	Verde

Comentario Riesgo	*Puntaje*
Bajo – Verde	0
Medio – Amarillo	5
Alto – Rojo	10
Severo – Negro	40

Riesgo Bajo	Es poco probable que exista mal uso de los recursos de los sistemas de información
Riesgo Medio	Podría dar lugar a un mal uso de los recursos de los sistemas de información si no es tratado adecuadamente.
Riego Alto	Generalmente es resultado de mal uso o tiene alta probabilidad de producir un abuso si no se corrige
Severo	Típicamente involucra fraude

Fuente: La Autora – COBIT

3.3 SOLUCIÓN PROPUESTA

No existe un Plan de Continuidad de negocios (BCP) para la unidad, por lo que en el caso de un desastre, la continuación de los procesos críticos de negocio puede estar en riesgo si los planes de la continuación del negocio no se completan.

Los procesos normales del negocio pueden verse afectados por los cortes extendidos del sistema informático o por no estar disponibles. El plan de continuidad de negocios ayuda en la continuación de las actividades críticas del negocio durante una interrupción causada por los desastres informáticos o no relacionados con la informática. Estos planes deben incluir actividades de contingencia para todos los procesos críticos de negocio en el caso de una interrupción en las operaciones comerciales normales o un corte de equipo extendido.

Se proponen las siguientes consideraciones:

Es necesaria la gestión adecuada de cada proceso crítico de negocio para la continuidad del mismo.

Realizar como parte del BCP el Plan de recuperación de desastres, enfocado en la restauración de los servicios de IT e infraestructura de la unidad.

Cubrir puntos de administración de riesgos como Seguridad de cuarto de servidores, instalar sistemas de detección y extinción de fuego, asegurar que el cuarto de servidores esté compuesto de materiales que contengan el fuego por al menos 1 hora, proveer de luces de emergencia, señalética en el caso de fallo de energía eléctrica, instalación de switch de control de energía desde donde pueda apagarse servidores y UPS al mismo tiempo.

Concentrar servidores e información crítica en los cuartos de servidores.

El entrenamiento formal debe ser coordinado con las partes principales del negocio para crear un estándar. El BCP debe tener en cuenta lugares como Quito, Carapungo, Guayaquil.

Este capítulo presenta la manera en la que se podrá implementar este proyecto en el mercado, combinando las herramientas administrativas y financieras para dicho fin.

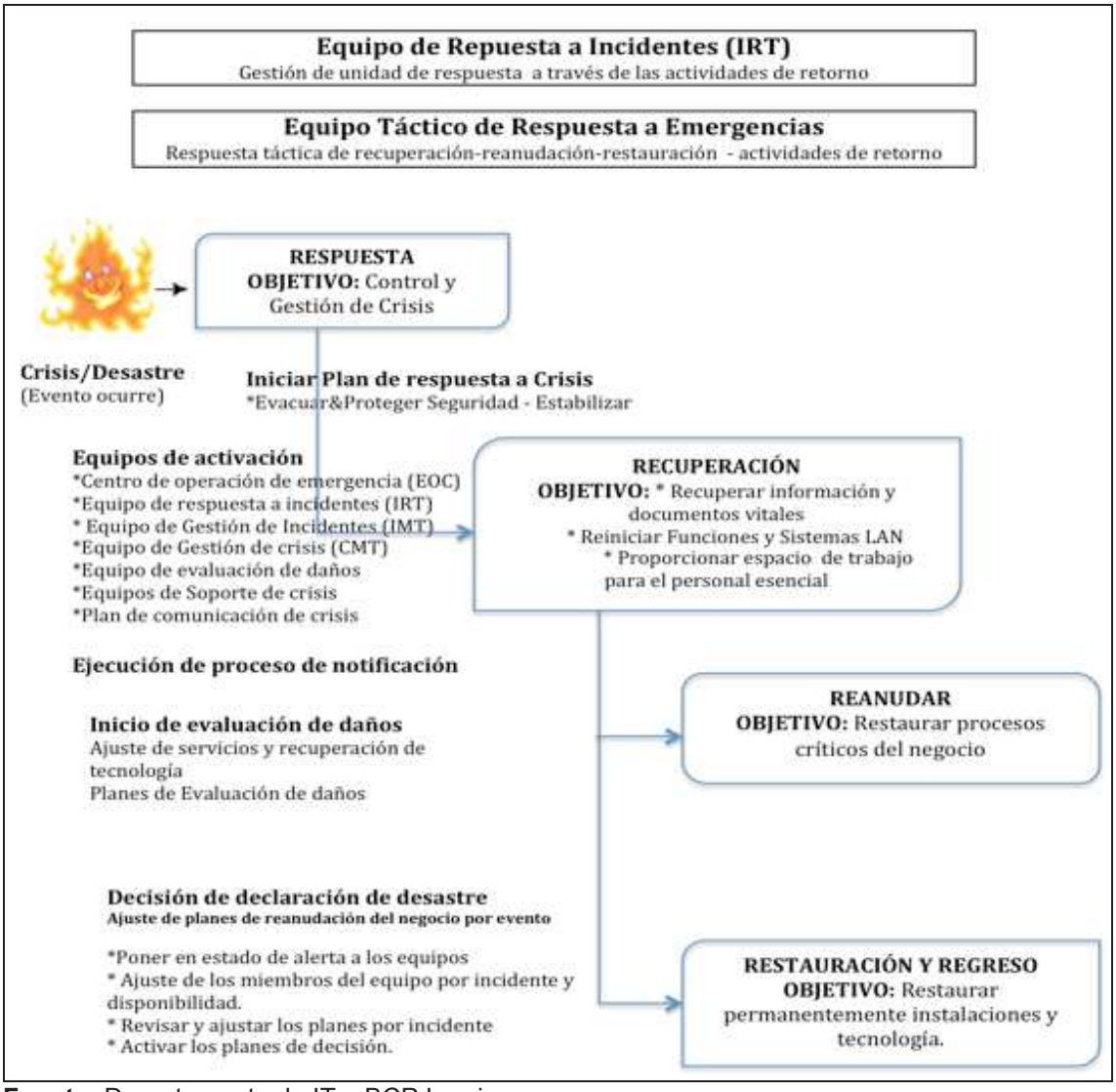
3.4 PLAN DE CONTINUIDAD DE NEGOCIOS PARA ISRARIEGO - ECUADOR

Versión 1.0 del (1, Marzo, 2011)
es aprobada por:
Gerente Operaciones
Gerente IT

3.5 INTRODUCCIÓN

Como se menciona en el marco teórico sobre las fases del BCP, a continuación se muestra el diagrama de flujo donde se esbozan los procesos y las actividades de respuesta que pueden ser usados cuando se trabaja con una crisis o emergencia.

Figura 3.1: Diagrama de Flujo de respuesta a emergencias



Fuente: Departamento de IT – BCP Israriego

3.6 PLAN DE RESPUESTA A CRISIS

Esta sección incluye las acciones de respuesta a los siguientes escenarios de crisis:

- Plan de Respuesta de Emergencia
- Plan del Equipo de respuestas a incidentes
- Centro de Operaciones de Emergencia y Logística

3.6.1 Plan de Respuesta a Emergencias

Esto será dirigido a Eventos mayores que afecten sistemas de tecnología, no incluye pandemia. Se ha establecido para las unidades de Quito, Carapungo y Guayaquil una Administración de emergencia.

Israriego ha considerado las situaciones potenciales de la emergencia que podrían presentarse en las unidades de Ecuador. Cada situación se trata a continuación, y se traza la respuesta a cada situación y los requisitos de los servicios de emergencia (ej.: Fuego, ambulancia, policía).

Las direcciones o ubicaciones físicas de Israriego son:

Israriego – Ecuador (Fábrica)
El Vergel No. 19 y Giovanny Calles
Sector de Carapungo, Quito Ecuador

Israriego – Ecuador (Area comercial)
Av. La prensa N2059 Y Manuel Valdivieso
Quito Ecuador

Israriego – Ecuador (Bodega)
Km 4 1/2 Vía Daule y Amadeo Moreira

El jefe de Calidad será responsable de dar mantenimiento a los procedimientos dentro del plan de emergencia. Las evacuaciones serán organizadas por la misma persona. Esto será anualmente y deberá ser registrado.

Existirá un delegado por cada unidad: Quito, Carapungo, Guayaquil.

Las responsabilidades de los encargados son:

- Asegurar que su área designada esté revisada y despejada.

- Reportar al encargado de la unidad o el vigilante al mando.

- Asegurar que las compuertas del sistema de fuego estén cerradas.

- Asegurar que todas las aplicaciones críticas estén cerradas.

- Asegurar que el listado de visitas haya sido extraído fuera de la oficina para tomar lista.

- Comunicarse con los bomberos de ser necesario.

- Todos los delegados deben recibir entrenamiento. Esto deberá llevarse a cabo en ambos casos con el personal de oficina y con los bomberos, estos entrenamientos deben ser documentados y cada empleado debe llevar su registro individual.

- En caso de emergencia en las oficinas Quito el punto de encuentro es: área de parqueadero.

En caso de emergencia en Carapungo el punto de encuentro es: Área 1 – puerta de salida 1, Área 2 – Puerta de salida 2.

a. Situaciones de Emergencia

Israriego ha determinado que las emergencias (potenciales) que existen son las siguientes y se manejarán en el lugar de trabajo:

- Fuego.
- Desastres naturales (ej. terremoto, ventarrones, tormentas, inundaciones
- Accidentes de primeros auxilios/Quemaduras
- Muerte

b. Procedimiento de Emergencia – Fuego

Empezará con alarma de fuego, ya sea por sirena o por anuncio del personal

- Llamada telefónica al 102.
- Solicitar servicios de bomberos
- Proporcionar las siguientes direcciones completas:

Quito:
El Vergel No. 19 y Giovanny Calles
Sector de Carapungo, Quito Ecuador
Teléfono: 593 2 2468 770

Carapungo:
El Vergel No. 19 y Giovanny Calles
Sector de Carapungo, Quito Ecuador
Teléfono: 593 2 2 822 995

- Permanecer en la línea para responder cualquier inquietud.

- Evacuar áreas de edificios. Lugar de encuentro para Quito es el área de parqueadero.

- Evacuar área de edificios. Lugar de encuentro para Carapungo: Área 1 – puerta de salida 1, Área 2 – Puerta de salida 2.

- Reunir al personal en las áreas designadas, los delegados deberán revisar el estado de cada persona.

- Los intentos para extinguir el fuego solo deben realizarse si las condiciones lo permiten.

- Los coordinadores de respuesta a emergencias o los delegados de la unidad debe ser quien advierta de la situación de emergencia, y provea mapas del sitio y toda la información que se requiera.

c. Procedimiento de Emergencia - Desastres Naturales

Terremoto, Ventarrones, Tormentas, Deslizamientos de tierra y otros desastres naturales.

El coordinador de respuesta a emergencias (Encargado de la unidad) deberá asumir autoridad y realizar lo siguiente:

- Evaluar la condición inmediata y la ubicación de todo el personal y hacer un breve registro de dicha información.

- Evaluar los daños evidentes y limitaciones a los edificios y / o servicios (sin poner en riesgo la seguridad personal)

- Notificar al personal clave y / o Servicios de Emergencia del Estado (SES) de nuevas directrices y, sobre todo en el caso de un aviso:

    - Contactar los Servicios de Emergencias del Estado
    - Consultar las últimas tres páginas en la guía telefónica
    - Escuchar la radio

El Coordinador de Emergencia debe garantizar que se mantenga el personal clave de referencia y la seguridad de todo el personal y los visitantes.

d. Procedimiento de Emergencia – Accidentes de Primeros Auxilios /Quemaduras

- Buscar un socorrista para evaluar la lesión.

- Si la lesión es una quemadura, ejecute la zona quemada con agua fría durante al menos 15 minutos. Esté atento a signos de shock.

- Si la lesión no es una quemadura, determinar si los primeros auxilios son adecuados o si la persona debe ser llevado a urgencias.

- Si es grave, llame a una ambulancia. Si no, llevarlos al hospital en vehículo o transporte.

- Proporcionar servicios de emergencia con datos personales de la persona lesionada (disponible desde el frente de disposición de personal).

e. Procedimiento de Emergencia – Muerte

Antes de entrar en el área de emergencia, prevenir de que es seguro hacerlo, y que no hay riesgo de daño físico.

No mueva a la persona, excepto en circunstancias extremas. Para ayudar a las investigaciones de accidentes, la escena debe permanecer tal y como fue cuando ocurrió el accidente. Si alguna parte de la escena debe ser movido, las fotografías de la escena antes de que se toca a facilitar las investigaciones.

Si hay alguna duda si la persona ha muerto, llame a una ambulancia en primer lugar. Ellos pueden ser capaces de revivir a una persona que parece estar muerto.

Si la persona es claramente teléfono fallecido, la Policía. Después de su llegada y evaluar la situación, que se llame a una ambulancia o el médico forense.

Proporcionar servicios de emergencia con datos personales de los heridos / persona fallecida (disponible desde el frente de disposición de personal)

f. Procedimiento de Eventos Adversos

El plan de respuesta ante eventos adversos y las responsabilidades del equipo de respuesta a emergencias se encuentra detallado en el Anexo 2 y 3.

3.6.2 Plan del Equipo de Respuesta a Incidentes (IRT - Incident Response Team)

Se ha realizado un estudio de la situación actual a fin de preparar a la Empresa para que pueda apoyar mejor a sus empleados y a sus familias, proteger su sólida reputación y mejorar sus posibilidades de sobrevivir a distintas situaciones de crisis. Después de analizar varias opciones, ISRARIEGO deberá adoptar un nuevo enfoque de respuesta a las crisis que incluye diferentes equipos.

Los equipos de respuesta a incidentes están compuestos por personas de un departamento o unidad comercial que responden a las crisis inmediatas.

El Equipo de Respuesta a Incidentes (IRT) es responsable de brindar una respuesta táctica e inmediata en el lugar de los hechos ante emergencias o incidentes. Puede existir más de un equipo de respuesta a incidentes de ISRARIEGO en una unidad o en un sitio. El Equipo de Respuesta a Incidentes puede tener la forma de un equipo de respuesta ante emergencias (es decir, el

equipo que responde ante emergencias de incendios, de seguridad o médicas) o de un equipo de respuesta funcional (por ejemplo, el equipo de respuesta de TI). La cantidad de miembros y la composición de los equipos de respuesta a incidentes variarán según el tamaño y la complejidad de la unidad, y también según los posibles riesgos que podrían afectar a la unidad.

A continuación se presenta el formato del listado de contactos IRT (Equipo de Respuesta a Incidentes) en el caso de un evento de emergencia de seguridad o, dependiendo de la situación, se podrá optar entre los planes descritos en el punto 1.1 (arriba) o en el Plan de Evacuación.

El listado IRT debe contener información sobre el cargo, el nombre y el teléfono de contacto.

Tabla 3.3: Listado IRT

Listado IRT		
Cargo	**Nombre**	**Teléfono de contacto**
Jefe Logística	Juan Pérez	9999-999

Fuente: La autora

a. Definición y funciones del IRT

El líder del equipo: El líder de IRT de la coordinación general de la reunión de IRT, la activación y el proceso de toma de decisiones. Las responsabilidades incluyen:

- Proporcionar una respuesta inmediata ante emergencias.
- Llevar a cabo la evaluación de los incidentes y determinar los recursos que son necesarios.
- Notificar al Equipo de Soporte Corporativo ante incidentes sobre la base de los umbrales de notificación.

- Mitigar la situación de emergencia.

- Asegurar que todas las actividades de gestión de crisis y comunicaciones sean coherentes con las políticas de la empresa y las regulaciones gubernamentales.

- Asegurar que las políticas de IRT y los procedimientos sean claramente definidos y que los miembros del equipo estén capacitados.

- Asegúrese de que se brindó capacitación a los nuevos integrantes sobre las funciones y responsabilidades de IRT.

- Mantener una lista de todos los contactos clave.

- Coordinar y difundir el calendario de reuniones en curso.

- Implementar planes de continuidad comercial o de retirada de productos.

- Restaurar las operaciones normales.

- Comunicarse con las partes afectadas y necesarias.

- Coordinar las comunicaciones públicas con el Departamento de Comunicaciones Corporativas.

- Gestionar la respuesta y la recuperación en el lugar.

- Garantizar que las actividades de respuesta en el lugar sean adecuadas.

b. Miembros del equipo:

Los deberes de los miembros de IRT son los siguientes:

- Dar prioridad a las responsabilidades de IRT las responsabilidades funcionales del día a día.
- Familiarícese con sus roles individuales, responsabilidades y procedimientos generales de IRT.
- Contribuir funcional experiencia y preparación para los esfuerzos de respuesta.
- Participar en su caso en el proceso de post-Incidente de Revisión.
- Participar en la formación de gestión de crisis y ejercicios.

3.6.3 Plan del Equipo Táctico de Respuesta a Incidentes TERT

"Equipo Táctico de respuesta a emergencias" (TERT) se refiere a aquellos equipos cuya misión es la de mitigar o eliminar un incidente o una crisis.

Ejemplos típicos de un equipo de respuesta a emergencias tácticas son "cuerpos de bomberos", "Médico de los Equipos de Respuesta", etc. TERTS proporcionar al grupo IRT de actualizaciones de estado en curso y ayuda a los equipos de respuesta para resolver la situación. Dependiendo del tamaño y complejidad, no puede haber muchos equipos tácticos de respuesta de emergencia en una unidad.

A continuación se detalla el formato del listado del TERT, debe existir uno por cada unidad, el listado debe detallar Cargo, nombre y teléfono de contacto.

Tabla 3.4: Listado TERT

Listado TERT		
Cargo	**Nombre**	**Teléfono de contacto**
Jefe Logística	Juan Pérez	9999-999

Fuente: La autora

La estructura de gestión de crisis de Israriego tiene tres niveles funcionales (ver figura 3-2).

Figura 3.2: Pirámide de Niveles Funcionales

Fuente: Departamento de Auditoría Interna – Israriego

El Equipo de Respuesta a Incidentes (IRT) y el Equipo táctico de respuesta a emergencias (TERT) son los grupos más operativos de la estructura de gestión de crisis y son responsables de actuar a nivel local en forma razonable en caso de un evento de emergencia, el nivel de Gestión Corporativa de Crisis son los directivos encargados de planificar y desarrollar el plan de seguridad.

3.6.4 Centro de Operaciones de Emergencia (EOC)

El Centro de Operaciones de Emergencia es el lugar donde la crisis de unidad o equipo de liderazgo de la organización gestiona la crisis. Este equipo de

liderazgo no es lo mismo que el Equipo de Respuesta a Incidentes o la táctica del Equipo de Respuesta de Emergencia que se mantiene en el lugar del evento participación en las actividades de respuesta y, en su caso, ayuda a las autoridades locales encargadas de las actividades de respuesta.

a. Ubicaciones del Centro de operaciones de emergencia EOC

En caso de un evento de crisis, el principal lugar EOC es Carapungo. La ubicación secundaria EOC es la Oficina Quito. En el caso de un evento de crisis en el sitio de Carapungo, el principal lugar EOC es Quito.

b. Plan de Operaciones del EOC

Véase el documento del Plan de Operaciones de Emergencia en el Anexo 4 en el cual se establecen los principios de funcionamiento, los procesos y la progresividad de un Centro de Operaciones de Emergencia.

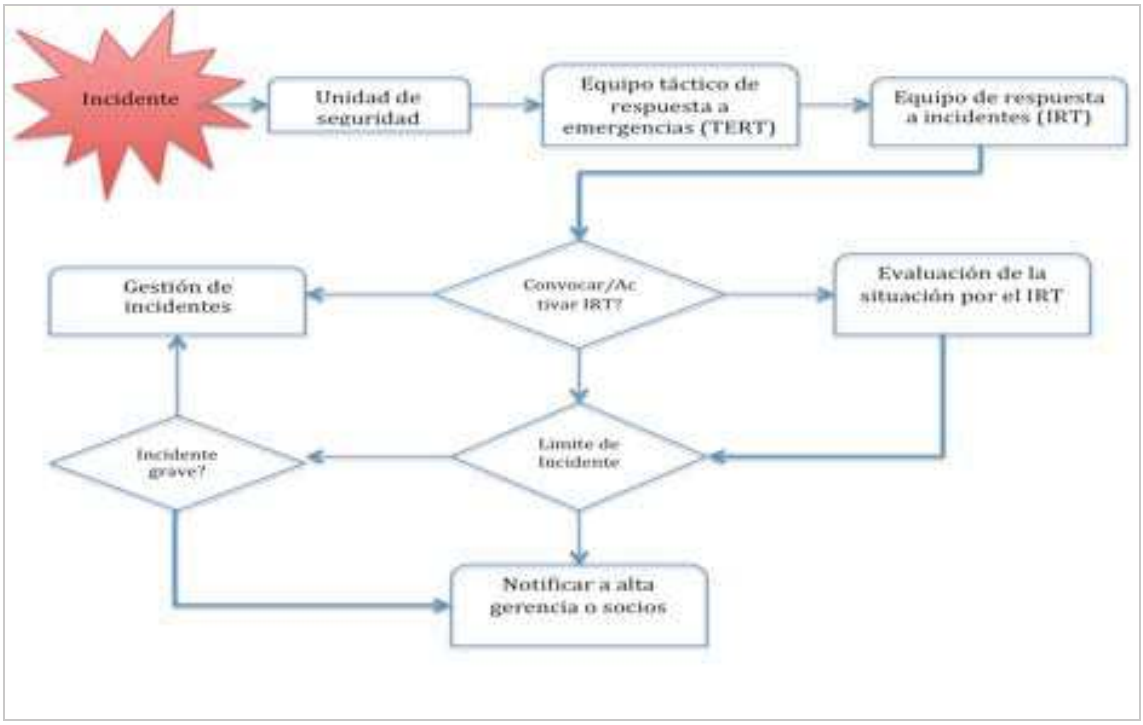
c. Plan de evacuación

El Plan de evacuación que Israriego se utilizará solo en el caso de emergencia. El proceso será gestionado por Recursos Humanos en cooperación con la gestión del ITR. Ver el Anexo 5 sobre el Plan Global de Gestión de Crisis.

3.7 PLAN DE COMUNICACIÓN DE CRISIS

El plan de comunicación de la unidad sigue básicamente el proceso de comunicación que se describe a continuación.

Figura 3.3: Flujo de Comunicación de Crisis



Fuente: Comité de BCP de Israriego

En el caso de un evento que tiene que ser reportado a nivel corporativo, se utilizará el siguiente proceso de apoyo de emergencia y comunicación.

Los Incidentes con alto nivel deben ser reportados al Centro de Seguridad.

Estos incidentes son:

- Cualquier víctima mortal relacionada con el negocio.

- Una amenaza para la salud o de negocios no relacionados con la empresa o evento reales que pueden afectar el funcionamiento del negocio a través de la ausencia significativa o distracción mental del trabajo (también conocido como un "evento de una pandemia").

- Acto de terrorismo o de tentativa de acto de terrorismo contra Israriego.

- Secuestro o intento de secuestro de un empleado de Israriego.

- Cometidos con bombas, secuestros o asesinatos que ocurren en las zonas donde opera Israriego.

- Actos reales o intento de espionaje contra Israriego.

- Interrupción debido a la pérdida de instalaciones, empleados, proveedores clave y / o de TI.

- Informe Nacional de los medios de comunicación o la investigación generada por un incidente que afecte a Israriego.

- Guerra de la revolución, conflicto armado o de acciones de la policía en los lugares donde el agua Israriego funciona o cuando el viaje empleados de Israriego.

- Identificación de los nuevos problemas que amenazan la imagen o reputación de Israriego.

- Inminente amenaza o amenaza real de un desastre natural en o cerca de un lugar de Israriego (incendios, terremotos, inundaciones, tormentas severas, tornados, huracanes).

- Demostración de activistas en las instalaciones.

- Trabajar en paro o bloquear la entrada de los empleados como resultado de cuestiones de trabajo.

- Medio Ambiente y los incidentes de transporte que resulta en daños para el medio público, la continuidad del negocio, daño a la imagen o la reputación de Israriego.

3.7.1 Plan de Comunicación de la Unidad

Esta sección contiene los planes y procedimientos para comunicar la información de eventos y crisis a personal de la unidad y los clientes externos e internos.

El Mapa de comunicaciones para interrupción de negocios se encuentra en el anexo 6.

El listado de verificación de crisis se encuentra en el anexo 7.

3.7.2 Notificación de Eventos, Guía de Contactos y Registros

Esta sección contiene las directrices de notificación y de contacto cuando se ocasiona un evento de crisis. A continuación se detalla el formato de registro de notificaciones y alertas de crisis.

Tabla 3.3: Formato de registro de notificaciones y alertas de crisis

Registro de notificaciones y alertas de crisis					
Nombre de quien realiza el llamado	**Fecha**	**Nombre de la persona llamada**	**Hora de llamada**	**Resultado de llamada**	**Detalles**

Fuente: Departamento de IT de Israriego

En el anexo 8 se detalla la comunicación a empleados de alerta de crisis.

3.7.3 Línea Telefónica de Interrupción de Negocio

Una línea telefónica de interrupción de negocios es un número especial donde se registra la organización / unidad de estado de las operaciones. Este es el número que los empleados llaman a averiguar si el establecimiento está abierto o no.

Línea telefónica de Israriego: (593-2) XXXX-XXX

3.7.4 Información de Contacto en Caso de Crisis

En caso de crisis, en el documento anexo se recogen todos los clientes clave críticos internos y externos, los principales proveedores y otros contactos para informar en caso de una interrupción del negocio.

Tabla 3.4: Formato de listado de contactos clave

Listado de contactos clave								
No. Vendedor	**Nombre**	**Calle**	**Ciudad**	**Región**	**Código Postal**	**País**	**Teléfono**	**Fax**

Fuente: Departamento de IT de Israriego

Tabla 3.5: Formato listado total de contactos

Listado completo de contactos								
No. Vendedor	**Nombre**	**Calle**	**Ciudad**	**Región**	**Código Postal**	**País**	**Teléfono**	**Fax**

Fuente: Departamento de IT de Israriego

El documento de primeros auxilios se encuentra detallado en el anexo 9.

3.8 PLANES DE RECUPERACIÓN

Esta sección contiene los planes para recuperar tanto la tecnología como la infraestructura de las instalaciones, los procesos críticos de negocio con el fin de activar sus planes de reanudación. Éste no es un estado “normal” de operación.

Los planes de restauración son los planes para restaurar la infraestructura y tecnología para volver al estado que estaba justo antes de la interrupción. Gran parte de este plan es escrito después que el evento ha ocurrido, que la evaluación de los daños se ha completado y que la decisión del liderazgo se ha

tomado en relación al nuevo estado. Lo que se puede planear de antemano son los equipos que estarán activos durante la restauración. Así como el diseño, el desarrollo y los planes de implementación que proveen continuidad dentro del tiempo de recuperación y de los objetivos del punto de recuperación.

3.8.1 Plan de Recuperación de Infraestructura de la Unidad

Los documentos con detalles de las instalaciones de Quito y Carapungo, edificios están ubicados en el anexo 10.

La información de activos detallados debe seguir la siguiente plantilla:

Tabla 3.6: Formato de listado de activos

Listado de activos					
Tipo de Activo	**Código**	**Detalle**	**Ubicación**	**Estado**	**Comentarios**

Fuente: Departamento Contable y Departamento de IT de Israriego

3.8.2 Plan de Recuperación de Desastres Computacionales (cDRP)

El enlace al CDRP delinea los planes para restaurar los procesos computacionales cuando haya fallos en el área de TI. El soporte a Israriego es realizado por el grupo de TI y está cubierto por el CDRP que este grupo estableció.

Este documento es el Plan de Recuperación de Desastres (DRP) para el Data Center de Israriego Cia Ltda., ubicado en Av. La Prensa N50-41, y Manuel Valdivieso, Quito - Ecuador. La presente información en este plan guía a la dirección de la empresa y al personal técnico del área de Sistemas en la recuperación de las funciones de procesamiento de los datos y servicios del área de Informática, en el caso de un desastre que destruya todos o parte de los recursos.

El Plan de Recuperación de Desastres está compuesto de un número de secciones que documentan los recursos y procedimientos a ser usados en la eventualidad que un desastre ocurra en las instalaciones del Data Center del área de Sistemas. Cada plataforma de procesamiento soportada tiene una sección específica, los procedimientos de recuperación. Existen también secciones que documentan el personal que será necesario para realizar las tareas de recuperación y una estructura organizacional para el proceso de recuperación.

El enfoque primario de este documento es proporcionar un plan para responder a un desastre que destruye o dañe severamente los sistemas de procesamiento centrales de la Organización operados por el área de Sistemas. El objetivo es restaurar las funciones de procesamiento tan rápidamente como sea posible, con los últimos y más actualizados datos disponibles.

El plan de CDRP se encuentra en el anexo 11.

3.8.3 Plan de Recuperación del área de Recursos Humanos

El plan de Recuperación del área de Recursos Humanos se enfoca en enlazar las posiciones existentes con las descripciones de trabajo. Éste identifica los requerimientos de recursos, habilidades, competencias y provee una referencia cruzada con la existente en el área de Recursos Humanos de Israriego la cuál puede ser utilizada.

3.8.4 Plan de Recuperación de Proveedores

Los siguientes datos deben presentarse en la información de proveedores

Tabla 3.7: Formato de listado de proveedores

Información de proveedores					
Proveedor	**Marca/Producto**	**Nombre**	**Dirección**	**Tlf Oficina**	**¿Critico?**

Fuente: Departamento de Logística de Israriego

3.9 PLANES DE REANUDACIÓN DE LOS PROCESOS DE NEGOCIO

Esta sección contiene los planes para la reanudación de los procesos críticos predefinidos de negocio que se ejecutarán luego de una interrupción de desastre.

Los Planes Individuales de Reanudación han sido desarrollados para cada área funcional. Estos deberían ser utilizados en una situación de crisis hasta que las operaciones normales hayan sido restauradas ver BIA por proceso.

3.9.1 Coordinadores de Continuidad del Negocio de la Unidad Listados por Proceso Crítico

La información necesaria de las personas quienes son responsables por el desarrollo, validación y puesta en marcha del mantenimiento de cada plan de Reanudación por proceso crítico se detalla a continuación:

Tabla 3.8: Formato de responsables del plan de reanudación

Responsables de plan de reanudación						
Proceso	**Unidad**	**Departamento**	**Apellido**	**Nombre**	**Teléfono**	**Email**

Fuente: Gerencia General de Israriego

3.10 PLAN DE EQUIPOS, ÁRBOL DE LLAMADAS Y ASIGNACIONES DE EQUIPOS

Los Equipos del Plan deben ser organizados por área funcional y por roles o posición y deben incluir las asignaciones de responsabilidad y de tareas. **Israriego– Ecuador** es una pequeña unidad de la compañía con sólo **XXX** posiciones permanentes. Por lo tanto, el equipo BCP no está separado del equipo IRT, y está compuesto por los mismos miembros quienes son responsables por el negocio. Una persona de cada área funcional está incluida en el equipo BCP y tomará responsabilidad por su área funcional. Los detalles

de contacto que incluyen número de teléfono laboral y teléfono celular están listados a continuación.

3.10.1 Tareas del Equipo por Posición

Facilitador BCP de la unidad:

Número de teléfono:
Número celular:

- Declara emergencia/Desastre
- Comunicarse con el IRT regional de Israriego (Estado, solicitud para decisiones, Resolución de problemas)
- Contactar a los miembros del BCP – Establecer el quipo
- Obtención emergente de autorización
- Reclamos y compensaciones
- Costo de seguimiento
- Responsable general para los arreglos H&S

Gerente de operaciones:

Número de teléfono 1:
Número de teléfono 2: +
Número celular:

- Co-coordina las actividades BCP
- Comunica las directivas a los miembros del equipo BCP
- Comunica los reportes de solicitudes/estados creados por el líder al equipo BCP
- Co-coordina las actividades del equipo BCP
- Maneja los problemas del personal
- Desarrolla y hace seguimiento al plan de acciones BCP

- Hace seguimiento del progreso y estado de las actividades operacionales afectadas
- Resume los reportes de estado BCP para posterior envío al Gerente BCP
- Aconseja al equipo BCP sobre los conflictos e incongruencias del plan de continuidad del negocio
- Acopia/registra toda la documentación relacionado a la reanudación/recuperación
- Documenta las actividades de reanudación/recuperación para las actualizaciones del plan
- Formalmente reporte y da por finalizado el BCP

Gerente de logística:

Número de teléfono 1:
Número de teléfono 2:
Número celular:

- Adquiere/mantiene las unidades físicamente
- Transporte/Acomodación
- Adquiere equipamiento y servicios de soporte
- Adquiere materiales de oficina/Alimentos/suministros médicos
- Operaciones del Centro de Operaciones de Emergencia (EOC).
- Adquiere los servicios externos

Gerente de comunicaciones:

Número de teléfono 1:
Número de teléfono 2:
Número celular:

- Medios de comunicación y comunicación externa
- Comunicaciones internas

Gerente TI:

Número de teléfono:
Número celular:

- Administración del Plan de Desastres de TI.

3.10.2 Lista de otros Contactos Clave

La siguiente tabla contiene la información necesaria de los contactos clave que debe ser notificado durante los cortes de energía y deben asegurar el soporte externo durante la reanudación de los procesos críticos.

Tabla 3.9: Formato de listado de contactos a ser notificados

Contactos a ser notificados			
Nombre	**Unidad**	**Teléfono**	**Celular**

Fuente: Comité de BCP de Israriego

3.11 APÉNDICES

Los apéndices consisten en documentos que soportan los sub-planes críticos de Continuidad del Negocio tales como Respuesta a Crisis, Recuperación de Desastres Computacionales y los planes de Reanudación de los Procesos Críticos de Negocio.

3.11.1 Respuesta a Crisis y Herramientas de Administración, Plantillas, Formularios

A continuación formularios y plantillas a ser usadas cuando se está respondiendo a una crisis, durante las actividades de valoración de los daños, para notificación de incidentes, procedimientos de comunicación, etc.

3.11.2 Criterios de Declaración de Desastres - Herramientas de Administración de Decisiones

La siguiente herramienta será de utilidad para valorar daños y realizar inventario de los mismos.

Tabla 3.10: Formato para inventario de daños

Criterio de declaración de desastres - Herramientas de decisión administrativa	
Perdida de personas claves	
Administrador	
Expertos en el área:	
No. Bajas	
No. Lesiones graves	
Fuera de servicio debido a circunstancias personales (familia afectada, pérdida de hogar)	
Pérdida de tecnología clave:	
Teléfono:	
Servidor local de archivos (daño físico):	
Infraestructura: sistema de cableado	
Virus: denegación de servicios	
Perdida del uso de la unidad:	
% de espacio perdido:	
Tiempo en el que el espacio no puede ser utilizado:	
Perdida de servicios públicos: luz, agua, teléfono	
Contaminación: tipo, alcance:	
Recursos locales de la comunidad que impiden el acceso o uso de las instalaciones (daños a carreteras, derrumbes, etc.)	
_____ Fecha: _____	
Firmar luego de ejecutar, notificar y entregar copia de este documento al equipo de Administración de crisis	

Fuente: Departamento de Auditoría y Administración de Israriego

3.11.3 Interrupciones del Negocio: Activación Telefónica - Formulario de Acción

Es necesario registrar el detalle de las llamadas de activación en caso de una interrupción del negocio, esta debe tener información del llamante, del receptor de llamada, datos de la llamada como fecha, hora, asunto a informar, quien recibe la llamada y de ser el caso a quien está asignada, razón, fecha y hora de la asignación.

Tabla 3.11: Formato de Listado de llamada de activación de interrupción de negocios

Interrupción de negocios – Llamada de activación							
Quien llama	**Llamada No.**	**Fecha y hora de llamada**	**Asunto**	**Recibida por**	**Asignada a**	**Como fue designada**	**Fecha y hora de asignación**

Fuente: Departamento de Auditoría y Administración de Israriego

3.11.4 Registro de Notificaciones a Contactos

El registro de notificación a contactos se encuentra en el Anexo 12

3.11.5 Formulario de Registro de Llamadas de Emergencia

El formulario de registro de llamadas de emergencia debe contener información sobre la hora y fecha de llamada así como un resumen de la misma. El detalle de la entidad a la que se informó la emergencia, el número y correo al que se contactó.

Tabla 3.12: Formato, Registro llamadas de emergencia

Formulario de registro de llamadas de emergencia							
Fecha/Hora/Registro llamada	**Registrado por:**	**Sinopsis de llamada**	**Nombre de Organización**	**Vencimiento**	**No. Teléfono - Fax**	**Email**	**Asignado a:**

Fuente: Departamento de IT de Israriego

3.11.6 Formulario de Evaluación de Daños

La información del formulario de evaluación de daños es utilizada luego del evento de crisis o emergencia, con el objetivo de evaluar la situación y recolectar información necesaria para la estrategia de recuperación.

Tabla 3.13: Formato evaluación de daños

Formulario de evaluación de daños	
Persona que informa el estado:	
Fecha y hora del reporte	
No Identificación	
1.- Describa el daño de equipos, indique detalladamente:	
2.- Proveea a detalle la ubicación del daño: Unidad, ubicación, piso, oficina:	
3.- Defina y estime el daño financiero del impacto al negocio:	
4.- Describa las alternativas posibles para continuar con el negocio activo:	
5.- Estime los recursos para la recuperación/restauración del negocio	

Fuente: Departamento de Administración de Israriego

3.11.7 Formulario de Informe de Evaluación de Daños

El informe de evaluación de daños es reportado con carácter urgente, debe contener el resumen del formulario de evaluación de daños.

Tabla 3.14: Formato informe de evaluación de daños

Fecha: Reportado po:				
Formulario de informe de evaluación de daños				
No. Identificación	**Fecha y hora de reporte**	**Persona que reporta el estatus**	**Describa el daño de equipos, provea detalles**	**Estatus actual**

Fuente: Comité de BCP de Israriego

3.11.8 Formulario del Centro de Operaciones de Emergencia

A. Checklist para activación o desactivación del EOC (Centro de operaciones de emergencia):

El listado de verificación contiene tareas a seguir para asegurar que todas las posiciones de emergencia puedan seguirlas según la fase activa.

Tabla 3.15: Formato verificación de activación EOC

Check list para activación o desactivación del EOC		
Para ser usado por todas las posiciones de las operaciones de emergencia	**Check**	**Remark**
Acciones de la fase de activación		
Contacte al equipo de seguridad		
Check in with Message Center and your function chair upon arrival at the EOC.		
Revise su área de trabajo y sus responsabilidades		
Revise sus recursos necesarios tales como fax, computador, copiadora, etc.		
Revise su checkist funcional.		
Retire o agrupe con cinta adhesiva todo cable que sea peligro de tropiezo		
Evaluar los niveles de dotación de personal para las tareas asignadas y comunicar las necesidades de Comandante de Incidentes (IC) o Líder de unidad de Equipo de Gestión de Incidentes (IMT.		
Establecer y mantener un registro cronológico de las actividades realizadas durante la crisis.		
Vista chaleco de colores según su grupo: OPS (naranja), Comandante (verde), Finanzas (amarillo), Centro de mensajes (blanco).		
Acciones de la fase de operación		
Informe a quien le releve, asegurar que está completamente informado de la situación actual antes de dejar el puesto o área de trabajo. Esto incluye cualquier clase de acción pendiente, su registro de acción y evento clave de información.		
Complete toda la información requerida, informes y cualquier otra documentación. Todos los formularios deben ser llenos antes de que abandone sus funciones.		
Deje limpia su área de trabajo antes de salir.		
Deje su número de teléfono de contacto para que pueda ser contactado en caso de ser necesario.		
Desactive la fase de activación – Cierre el EOC		
Desactive su posición de trabajo y cierre su registro de actividades cuando tenga la autorización del líder del IMT.		
Regrese a sus actividades normales.		
Provea copias de todas las actividades, documentos, registros y otros que haya realizado bajo su cargo de emergencia.		
Ayude o asista al informe del EOC y esté listo para dar retroalimentación.		

Fuente: Departamento de IT de Israriego

B. Notificación inicial:

La notificación inicial es realizada a todos los contactos de la empresa, el registro debe contener información de la persona que realiza la llamada como la que la recibe, así como la hora, fecha y resultado de la llamada.

Tabla 3.16: Formato de registro de notificación

Alerta de crisis y registro de notificación a contactos					
Empleados llamados por:	***Fecha***	***Nombre de persona llamada***	***Hora de llamada***	***Resultado de llamada***	***Comentarios***

Fuente: Comité de BCP de Israriego

3.11.9 Reporte de Incidentes

El reporte de incidentes permite responder a los mismos de forma sistemática facilitando la recuperación de las actividades del negocio.

Tabla 3.17: Formato de reporte de incidentes

Formulario de reporte de incidentes							
Persona que llama	**Fecha y Hora**	**Descripción del incidente**	**Persona que recibe llamada**	**Designado a:**	**Responsable**	**Estado**	**Comentarios**

Fuente: Comité de BCP de Israriego

3.11.10 Directrices y Procedimientos

Tabla 3.18: Formato de activación de Equipo de respuesta a crisis

Paso	*Acción*	*Información de alerta*
1	Escribir el nombre, título y número de teléfono de la persona que será notificada por usted cuando la decisión de declarar una situación de desastre ha sido tomada	Nombre: XXXXXXXXXX Título: XXXXXXXXXX Teléfono #: XXXXXXXXXX
2	Cuando y donde van a reunirse en la primera acción de respuesta, recuperación o reanudación. Esta debe ser un área de montaje y no en el área de recuperación o en una ubicación alterna al lugar de trabajo.	Ubicación: XXXXXXXXXXX Tiempo: XXXXXX Número de contacto: XXXXXXXX
3	Ubicación del área alterna de trabajo o de recuperación si no corresponde a la descrita en el cuadro de arriba.	Ubicación: XXXXXXXXXXX Número de contacto: XXXXXXXX
4	Confirmar de antemano los arreglos de transporte para los empleados y materiales de recuperación, en el caso que el equipo necesite movilizarse a una ubicación alterna.	
5	Asegurarse de poseer una copia del BCP de la unidad. Si no, determine de dónde puede obtener una copia.	
6	Luego que su equipo haya sido activado, los integrantes deben contactar a sus familias si una emergencia familiar ocurriera. Establezca un número de contacto único y provéalo a los miembros de su equipo.	Número de contacto: XXXXXXXX XXXXXXXXXXX
7	Notifique a su equipo que un desastre ha sido declarado y dónde deberían reunirse.	Ubicación: XXXXXXXXXXX Número de contacto: XXXXXXXX

Fuente: Comité de BCP de Israriego

Procedimiento de Activación de Equipo de respuesta a crisis.

Debe existir una lista de personal autorizado quienes puedan declarar un incidente o evento de desastre. La lista debería estar en orden de prioridad y debe incluir nombre, título, descripción y número(s) de contacto.

El equipo líder que decide la declaración de una situación de desastre debe encargar a una persona para que recomiende a todas las partes importantes interesadas, incluyendo el Líder del Equipo identificado en el Plan de Respuesta a Crisis, que un desastre ha sido declarado. Los líderes del equipo deben asegurarse que ellos tengan toda la información que necesiten para empezar sus procedimientos de activación de quipo. La tabla 3.19 puede ser utilizada para recopilar la información necesaria.

3.11.11 Cronograma del Mantenimiento del BCP de la Unidad

En la siguiente tabla se encuentran los pasos a seguir en orden de actividad para realizar el mantenimiento del BCP y su periodicidad.

Tabla 3.19: Cronograma del mantenimiento del BCP de la unidad

	Artículos del plan de mantenimiento	Responsabilidad	Cronograma
1	Mantenimiento del directorio BCP en el servidor local de la unidad. Los subdirectorios deben ser: Business Impact Analysis (BIA) Operacional Financiero RRHH Plan de respuesta a crisis Plan de respuesta a emergencias Plan de operaciones de seguridad Plan de respuesta Plan de comunicación Plan de recuperación y restauración Recuperación IT (Disaster recovery Plan) BIA (por procesos esenciales)	Coordinador BCP de la unidad	En el curso
2	Llevar a cabo las revisiones del subplan para evaluar su precisión. Los dueños del subplan y del plan de reanudación son responsables del mantenimiento de sus planes y de notificar al coordinador BCP de la unidad de los cambios realizados. Cuando algún cambio en el proceso ocurra, se debe evaluar si el cambio propuesto o planificado impactará en el BCP de la unidad. Si es así, se debe actualizar el subplan en paralelo con los cambios implementados.	Gerente IT de la unidad, dueños del subplan y los Coordinadores de continuidad del Negocio (Dueños del negocio)	Anual
3	Revisar el Plan CDRP evaluando la precisión de la información. Actualizar cuando sea apropiado.	Gerente IT de la unidad	Cada dos años
4	Llevar a cabo la validación de los ejercicios de evacuación y refugio en sitio. Árbol de llamadas Ejercicios prácticos de Gestión de Crisis	Coordinador del BCP de la unidad, supervisor de la unidad	Cada dos años
5	Llevar a cabo un tipo de simulación de los ejercicios del plan CPR que el equipo requerirá para reconstruir los servidores de archivos de la unidad que contienen la información requerida para rápidamente reanudar los procesos de negocio esenciales. Medir los resultados de acuerdo a los RTO y RPO.	Gerente IT de la unidad	Anual
6	Llevar a cabo los ejercicios de entrenamiento con los miembros del equipo proveyendo de la práctica que ellos necesitan para cumplir efectivamente con las tareas de reanudación y con los procedimientos, para que estén preparados en casos reales.	Coordinador del BCP de la unidad y líderes de Equipo	Anual

Fuente: Comité de BCP de Israriego

3.11.12 Plan de Mantenimiento del BCP de la Unidad

Revise el punto 3.11.11 Cronograma de mantenimiento BCP de la Unidad

3.11.13 Plan de Distribución de BCP

Una copia impresa de las secciones de trabajo del BCP de la unidad deben ser distribuidas al menos a:

- El líder del equipo, reemplazos y alternos del Equipo de Respuesta Incidentes (IRT)

- Todos los Líderes del Equipo, reemplazos y alternos.

- Ubicaciones de custodia fuera de sitio

Para asegurarse que los destinatarios poseen la última versión oficial de las secciones del plan y de la documentación, la distribución será controlada por el Coordinador BCP de la Unidad. Se recomienda que, al menos, los destinatarios sean proveídos de las últimas versiones de los siguientes documentos:

- Un cronograma de actividades de mantenimiento, y/o

- Una actualización que es el resultado de un Evento de Cambio de Control

Adicionalmente, para los destinatarios de la copia impresa del plan oficial, se recomienda que el Coordinador BCP notifique a los destinatarios que recibirán la última versión de su plan dentro de los siguientes días, y que hagan la solicitud en la oficina para que las páginas con actualizaciones de su carpeta BCP puedan ser reemplazadas.

3.11.14 Contactos de Distribución

El listado de contactos de distribución contiene el cargo y nombre del personal asignado.

Tabla 3.20: Listado de Contactos de distribución del BCP

Título/Cargo	*Nombre*
Gerente de Operaciones y Cadena de Suministros	
Gerente de Recursos Humanos	
Jefe de TI	
Jefe de Calidad (Coordinar BCP de la unidad)	
Controller	
Director Regional, Gerente de Operaciones y Suministros	
Gerente de la Plataforma BCP	

Fuente: Comité de BCP de Israriego

3.11.15 Análisis de Impacto al Negocio, Planes de Recuperación

El proceso de análisis de impacto al negocio y su proceso de recuperación de cada área crítica establecida por los directivos de la empresa se encuentran en los anexos 13 y 14.

3.11.16 Prioridades de Procesos Críticos y RTO

El siguiente cuadro detalla el tiempo de recuperación de cada proceso crítico establecido por los directores de la compañía.

Tabla 3.21: Procesos y sus tiempos de recuperación

Proceso	***Prioridad***	***RTO***
Producción y logística		
Proveeduría	2	Días
Producción	1	Días
Finanzas y contabilidad		
Control de fondos	3	Días
Recursos Humanos		
Proceso de contratación	4	Días

Fuente: Comité de BCP de Israriego

3.11.17 Evaluación de Riesgos

Tabla 3.22: Evaluación de riesgos de ISRARIEGO CIA. LTDA.

Edición original		Autorizado por	
Revisión #:	0		Gerente de Operaciones
# Pág:	1		

Hoja de evaluación de riesgos

Esta hoja de trabajo considera muchas variables para facilitar la prioridad de rango de los riesgos o amenazas. Para utilizar esta hoja de trabajo, la lista de los riesgos a la izquierda y usar la fórmula como se indica en los títulos de las columnas para formar la relación con respecto a todos los otros riesgos. Añadir otros riesgos o amenazas que se consideren necesarias. Confíe en su propio juicio para su departamento o centro de conjunto de los riesgos. Ver los resultados del peso relativo calculado para cada una de las amenazas y considerar la mitigación de los riesgos más probables que tienen el mayor impacto. Esta tabla amenaza / vulnerabilidad representa riesgo, la probabilidad y el impacto utilizando un método de comparación relativa.

El cálculo es: La probabilidad multiplicado por la suma de los cuatro factores de riesgo multiplicado por el impacto el resultado es el **peso relativo**

Mientras mayor sea el peso relativo, mas crítica será la estrategia de mitigación.

Unidad	Israriego												
			Factores de riezgo										
AMENAZA O RIESGO	Probabilidad	X	(Velocidad de Inicio	+	Preaviso	+	Duración	+	Intensidad)	X	Impacto	=	Peso relativo
Terremoto	2		2		1		1		2		3		36
Fuego	2		2		2		1		2		2		28
Fallo en sistema principal Software /Malfuncionamiento	2		2		2		1		1		2		24
Fallo en sistema principal Hardware /Malfuncionamiento	1		2		1		2		2		3		21
Pérdida de personas clave	1		2		2		2		1		2		14
Falla en sistema de backup	1		1		2		2		1		2		12
Erupción volcánica	2		1		1		2		2		1		12
Corte de Energía Eléctrica	2		1		1		2		1		1		10
Interrupción LAN	1		1		2		1		1		2		10
Derrame Químico	1		2		2		1		1		1		6
Tormenta eléctrica	1		2		1		1		1		1		5
Inundación	1		1		1		1		1		1		4
Sistema de fallo en principales sistemas	1		1		1		1		1		1		4
Amenaza de bomba	1		1		1		1		1		1		4
Explosión	1		1		1		1		1		1		4
Sabotaje humano	1		1		1		1		1		1		4

Definiciones	Valores	Descripción
Probabilidad	1=Baja 2=Media 3=Alta	Probabilidad relativa que el evento suceda.
Velocidad de inicio	1=Lento 2=Rápido	Tiempo transcurrido entre la primera advertencia y el inicio del evento.
Preaviso	1=Suficiente 2=Insuficiente	El primer aviso con suficiente antelación para permitir todas la medidas de mitigación
Duración	1=Corta 2=Larga	La duración prevista del evento (no el resultado)
Intensidad	1=Baja 2=Alta	El nivel de intensidad que se impondrá durante el evento
Impacto	1=Baja 2=Media 3=Alta	El impacto que es probable que continúe como consecuencia del evento

Fuente: Comité de BCP de Israriego

3.12 REGISTRO DE ADMINISTRACIÓN DE CAMBIOS

La siguiente tabla de registro de cambios contiene información sobre los cambios realizados al plan, así como el detalle del cambio, fecha, persona que realiza el cambio y la versión asignada al documento.

Tabla 3.23: Registro de administración de cambios

Registro de Administración de Cambios			
Descripción del cambio	**Nombre**	**Fecha**	**Versión**

Fuente: Comité de BCP de Israriego

3.13 PLAN DE PRUEBAS

Los planes de continuidad del negocio deberán ser probados y actualizados regularmente para asegurar que sean actuales y efectivos.

3.13.1 Lineamiento de Implementación

Las pruebas del plan de continuidad del negocio deberán asegurar que todos los miembros del equipo de recuperación y otro personal relevante estén al tanto de los planes y su responsabilidad con la continuidad del negocio y la seguridad de la información, y que conozcan su papel cuando se invoque el plan.

El programa de pruebas para el plan de continuidad deberán indicar cómo y cuándo se deberá probar cada elemento del plan. Cada elemento del plan deberá ser probado frecuentemente:

- Prueba flexible de simulación (*table-top testing*) de varios escenarios (discutiendo los acuerdos de recuperación comercial utilizando ejemplos de interrupciones);

- Simulaciones (particularmente para capacitar a las personas en sus papeles en la gestión post-incidente/crisis);

- Prueba de recuperación técnica (asegurando que los sistemas de información puedan restaurarse de manera efectiva;

- Prueba de recuperación en el local alternativo (corriendo los procesos comerciales en paralelo con las operaciones de recuperación lejos del local principal);

- Pruebas de los medios y servicios del proveedor (asegurando que los servicios y productos provistos externamente cumplan con el compromiso contraído);

- Ensayos completos (probando que la organización, personal, equipo, medios y procesos puedan lidiar con las interrupciones).

3.13.2 Formulario de Retroalimentación del Participante

Parte I – Recomendaciones y pasos de acción
Nombre del ejercicio: _____ Fecha del ejercicio: _____
Nombre del participante: _____ Cargo: _____
Acción: _____ Rol: __ Jugador __ Facilitador __ Evaluador __ Observador

Basado en el ejercicio de hoy liste las 3 áreas que fueron más exitosas.

Basado en el ejercicio de hoy liste las 3 áreas que necesiten mejora.

Identifique los pasos de acción que deben ser tomados en cuenta para los dos puntos nombrados anteriormente.

Describa los pasos de acción que deben ser tomados en cuenta en su área de responsabilidad. ¿Quien debe ser nombrado responsable por cada acción?

Liste el equipo, entrenamiento, planes o procedimientos que deben ser revisados o desarrollados. Indique el nivel de prioridad de cada uno.

Parte II – Diseño de ejercicio y conducta

¿Cual es su evaluación del ejercicio?

_____

Por favor califique en la escala del 1 al 5, siendo 1 descuerdo y 5 de acuerdo.

	Factor de calificación	**Calificación de satisfacción**				
a.	El ejercicio estuvo bien estructurado y organizado.	1	2	3	4	5
b.	El escenario del ejercicio fue real y plausible.	1	2	3	4	5
c.	La documentación utilizada durante el ejercicio fue un instrumento valioso a través de todo el ejercicio.	1	2	3	4	5
d.	La participación en el ejercicio fue apropiada para cualquier persona en mi posición.	1	2	3	4	5
e.	Los participantes incluyeron a la gente correcta en términos de nivel y mezcla de disciplina.	1	2	3	4	5

¿Que cambios haría usted para mejorar el ejercicio?

Por favor provea cualquier recomendación sobre como este o futuros ejercicios podrían ser mejorados.

_____

3.13.3 Lista de Verificación del Evaluador

Evaluador: _____ Fecha: _____

Ubicación: _____ Escenario: _____

Objetivos: _____

Tabla 3.24: Encuesta de evaluación de pruebas

	S	N	NA	NO
1. Plan contenía un procedimiento para la activación de IRT en esta situación				
2. Plan contenía un lugar alterno de trabajo				
3. Los miembros del IRT tenían los recursos de comunicación a la mano para emergencias (información de contactos de empleados, información de contactos de emergencia, etc.				
4. El IRT tiene planes para manejar los medios de comunicación				
5. El IRT dirigió la activación de los planes recuperación y reanudación.				
6. El IRT manejó este evento como grave y lo notificó al CIST.				

Fuente: Comité de BCP de Israriego

Por favor responda: S=Si, N=No, NA=No Aplica, NO=No observado

3.13.4 Formato de Reporte después del Evento

Nombre del evento: _____ Fecha: _____

Unidad: _____

Coordinador del BCP: _____

Nombre del líder del IRT: _____

Fecha de la revisión del Post Incidente: _____ (dd/mm/yyyy)

Fortalezas comunes identificadas durante el evento:

_____

Debilidades comunes identificadas durante la revisión del evento:

_____

Recomendaciones de la revisión del evento:

Desde la lista de recomendación, por favor liste los que tendrán seguimiento como acciones de mejora.

Tabla 3.27: Lista de recomendaciones para pruebas

Acción recomendada	Fecha propuesta de termino	Persona asignada

Fuente: Comité de BCP de Israriego

3.14 CERTIFICACIÓN DEL PLAN

3.14.1 Checklist de Visto Bueno para Aprobación del BCP

El requisito mínimo a quien se le realizarán las preguntas del checklist es el Gerente de la unidad a través de quien se coordinarán los informes del BCP.

Tabla 3.28: Lista de revisión para aprobación del BCP

	Plan BCP – Confirmar:	√	***Comentarios***
1.	Existe un análisis del impacto en el negocio (BIA) que define aplicaciones criticas, procesos, funciones y registros vitales.		
2.	Existen checklists, listas de acción, y/o procedimientos operacionales estándar (SOPs) que identifican asignaciones de emergencia, responsabilidades y lugares de destino de emergencia.		
3.	Existe una evaluación del riesgo documentado por natural, hecho por el hombre y riesgos tecnológicos.		
4.	Existen prioridades de términos cortos y términos largos plazos para restauración de la operación del negocio.		
5.	Los BCP identifican y documentan las partes interesadas que deben ser notificadas antes, durante o después de una emergencia /desastre / interrupción		
6.	Existe documentación de la ubicación de los sitios de trabajo alternativos previstos.		
7.	Los documentos del plan BCP y procedimientos para asegurar la protección del personal, instalaciones y recursos, de manera que la entidad pueda funcionar con eficacia.		
8.	Existe un cronograma de distribución documentado que identifica a las personas que reciben copias actualizadas de los BCP.		
9.	Un Coordinador de BCP se le ha asignado y autorizado por la dirección de la unidad para administrar y asegurar que el plan se mantenga al día.		
10.	La unidad ha llevado a cabo en la instrucción o el ejercicio anual de su plan de BC (s) que incluye un plan de acción correctiva para corregir las deficiencias.		
11.	El plan contiene una lista de proveedores, incluyendo proveedores alternativos para la adquisición de los recursos durante una interrupción importante.		
12.	El Plan identifica las principales y suplentes de los lugares de Centro de Operaciones de Emergencia.		
13.	Existen procedimientos para asegurar la selección, conservación y disponibilidad de los documentos esenciales para el funcionamiento efectivo de la entidad, en condiciones de emergencia y para mantener la continuidad de las operaciones.		
14.	Existe un plan de equipo de respuesta a incidentes (IRT).		
15.	Existe un plan de respuesta ante una pandemia		
16.	El plan ha sido firmado por el coordinador del BCP y la unidad de la alta dirección.		
17.	El plan es realista y efectivamente asegura la gestión de una interrupción de la actividad / incidente de emergencia y operaciones de negocio sostenible en el futuro.		

Fuente: Comité de BCP de Israriego

3.14.2 Acta de Acuerdo y Certificación de Revisión del BCP

Certificación del Plan de Continuidad de negocios para **Israriego**

Yo/nosotros certificamos que el anterior plan de referencia de continuidad del negocio está alineado Israriego, a los estándares de continuidad de negocio de la empresa y contiene todos los elementos necesarios para recuperarse y reanudar los procesos críticos de negocio y funciones dentro de determinados objetivos de tiempo de recuperación después de una interrupción significativa en el negocio.

_____	_____	_____
Nombre	Firma	Fecha

_____	_____	_____
Nombre	Firma	Fecha

Este documento está destinado para el uso de la alta dirección, administración, propietarios de procesos de negocio, sujetos de la materia y expertos técnicos, y personal de continuidad del negocio que interactúan con esta unidad.

CAPITULO IV

4 CONCLUSIONES Y RECOMENDACIONES

Después de haber realizado el plan de continuidad de negocios completo se pudo llegar a las siguientes conclusiones y recomendaciones.

4.1 CONCLUSIONES

Debido a la definición de BCP, el alcance de esta tesis ha cubierto todas las áreas del negocio no solamente IT en vista de que en manejan información crítica para la continuidad del negocio, el BCP fue desarrollado mediante el análisis de proceso críticos junto con los directivos de la unidad. Se pudo determinar que el enfoque de BCP está directamente relacionado con las necesidades de la empresa garantizando así la continuidad de los procesos elegidos.

El BCP desarrollado enfoca sus esfuerzos para asegurar cuatro pilares específicos que son; personal humano, proveedores y clientes, IT y operaciones. Debido a esto se considera eficiente puesto que ayudará a mitigar los eventos de los riesgos operacionales.

Después de la implementación del BCP, la compañía está en capacidad de responder ante una situación de desastre de gran impacto en sus actividades.

Se han seleccionado amenazas de acuerdo a la mayor probabilidad de ocurrencia y de mayor impacto potencial. Estas fueron todas determinadas de acuerdo con las características del negocio y de esta forma se identificaron los efectos potencialmente negativos por medio de estrategias y acciones a seguir para la recuperación de la operaciones críticas de la unidad, contrarrestando las interrupciones de los proceso principales del negocio.

Luego del desarrollo del BCP se concluye que este proceso es de continua planificación, prevención, educación constante y pruebas que demuestren la efectividad del mismo, todos los procesos de respuestas son sujetos a auditorías que deben realizarse anualmente.

El plan se desarrolló en base a estándares internacionales presentando los procesos de recolección y análisis de información así como la aplicación de principios necesarios para una adecuada gestión de la continuidad del negocio que cubre las necesidades de clientes y organizaciones, basado en un Sistema de Gestión de Riesgos.

Se ha recuperado la información necesaria para el BCP focalizándose específicamente en la recolección de las funciones y sistemas críticos determinando amenazas primordiales de acuerdo a las características del negocio, siguiendo de esta forma la metodología planteada.

Los procesos críticos se identificaron realizando un mapa de procesos misionales, críticos y de apoyo, documentando los procesos seleccionados indicando en cada actividad o tarea el apoyo de TI las interfaces o interdependencias así como de los controles existentes.

4.2 RECOMENDACIONES

Es vital mantener los procesos actualizados y vigentes por lo que se propone revisiones trimestrales de los procesos que a su vez deberán actualizar los planes y procedimientos del BCP.

Se recomienda realizar mantenimiento al BCP por medio de revisiones periódicas del análisis de impactos y riesgos del negocio, planes de recuperación y árbol de llamadas.

Se sugiere realizar un levantamiento y documentación de los procesos críticos de las áreas de: Recursos Humanos y Producción y de los no críticos como ingreso de información, facturación y emisión de reportes para la toma de decisiones, con el fin de facilitar el relevo de actividades en casos de emergencia o pérdida de personas clave.

En el siguiente año será necesario implementar en la red un proceso de escalamiento de equipos de red y software de control, que permita actualizar los sistemas e introducir nuevas tecnologías que faciliten segmentar la red de tal forma que se pueda brindar mayor seguridad a la misma.

Se recomienda la implementación de seguridades en el cuarto de servidores tales como sistema de aspersión, cambio de piso, instalación de master power switch debido a que tales falencias de seguridad física debilitan la seguridad de la información.

Se sugiere que por medio de políticas claras sobre el uso de grupos de acceso a información se implementen controles en los accesos. La ausencia de políticas al respecto genera una gran debilidad en la protección de información.

BIBLIOGRAFÍA

- BRITISH STANDAR INSTITUTE, BS-25999 Plan de Continuidad del Negocio – DRI, (2007). Barcelona,España (2da parte).

- COBIT IMPLEMENTATION, Organización del área informática, Recuperado el 29 Junio 2011 de http://www.isaca.org

- ESA Security, Certificación de la gestión de riesgos, Recuperado el 20 de mayo de 2011, de http://www.esa-security.com/web/servicios/index.htm

- ISEC, Sixto Flores (2010) – Conceptos BCP – Administración de la Continuidad de los Negocios - Sistema de Gestión de Continuidad de Negocios.

- MAGERIT, Metodología de Análisis y Gestión de riesgos de los sistemas de información, http://publicaciones.administracion.es, 2008, Fecha de consulta (10-09-2011), Madrid, España de Catálogo general de publicaciones oficiales.

- MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT). Tomo I:Método. Ministerio de Administraciones Públicas, Madrid 2006.

- MAGERIT, Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

- SYED, Akhtar, Syed Bmath Afsar, Business Continuity Planning Methodology, 2004.

- UNE, ISO/IEC 17799, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de gestión de la seguridad de la información.

- UNE, ISO/IEC 2700, (2005). Sistemas de Gestión de la Seguridad de la Información (SGSI). Madrid, España: Ed. AENOR 2007.

- UNE, ISO/IEC 27001, (2007). Sistemas de Gestión de la Seguridad de la Información (SGSI) 1era Modificación. Madrid, España: Ed. AENOR 2009.

ANEXOS

ANEXO 1

GLOSARIO

Activación: La reunión formal inicial del equipo (CIST o CCMT) que marca el comienzo del proceso corporativo de toma de decisiones y de respuesta a la crisis; el equipo asume su autoridad en virtud de este Plan Global de Gestión de Crisis.

Interrupción comercial: La interrupción de un proceso comercial, producción, servicios y/o entrega al punto que dañe la estabilidad financiera del negocio o la posición en el mercado de la organización que participa en el proceso comercial.

Reunión: La primera reunión física o virtual del equipo (CIST o CCMT) para llevar a cabo un análisis inicial de un incidente que se ha informado y para determinar si se necesita la activación formal del equipo u otra acción corporativa.

Crisis: Un suceso extraordinario que puede poner en peligro la vida de los empleados, interrumpir las operaciones o afectar gravemente la solidez financiera o la imagen pública de la Empresa.

Emergencia: Toda situación, real o inminente, que ponga en peligro la seguridad, la integridad y el bienestar de los empleados, clientes, visitantes y propiedad de ISRARIEGO, además del medioambiente.

Problemas emergentes: Un problema o una serie de incidentes aparentemente inconexos que pueden generar noticias negativas o dañar la reputación si se hacen públicos y que puedan tener como resultado multas, resarcimiento por daños y perjuicios, gastos no calculados en el presupuesto y

otros costos (por ejemplo, defectos del producto, fallas de diseño, ética comercial) que superen la cantidad determinada previamente.

Incidente: Un suceso, una serie de sucesos o un conjunto de circunstancias que interrumpen los procedimientos operativos normales.

ANEXO 2

PROCEDIMIENTO DE ADMINISTRACIÓN DE EVENTOS ADVERSOS

1. Evacuación

En cualquier evacuación, el personal determinado adoptará las funciones de Delegado de Unidad, Delegado encargado de Unidad y de Vigilantes de la zona. Vigilantes de la zona son los responsables de la evacuación de un determinado nivel o área del edificio. El Delegado de Unidad y su Adjunto coordinarán la evacuación y el contacto con personal de Servicios de Emergencia. Durante la evacuación, Los vigilantes tienen plena autoridad sobre todas las personas en y cerca del edificio. Los vigilantes se identifican con los "cascos" de color blanco el Delegado de Unidad y su suplente, rojo para el Área de Vigilantes. Después de 4 horas, el supervisor de turno cumple el papel de Delegado.

La evacuación de los edificios normalmente se iniciará con la activación de las alarmas de evacuación del edificio, ya sea manual o automáticamente. Cuando el sistema de alarma de evacuación falle o en alguna situación de emergencia, el comando de evacuación será propuesto por el Delegado de Unidad y/o su encargado, o el personal de Servicios de Emergencia, y puede ser transmitida por el Delegado, un funcionario u otra persona a la que se le da autoridad para hacerlo.

Cuando la evacuación del edificio se ha iniciado el procedimiento de la compañía es el siguiente, (a menos que las circunstancias requieren un arreglo).

(1) Mantenga la calma y el cese de las actividades.

(2) No recoger objetos personales.

(3) Salga del edificio por las rutas de evacuación designadas o como dirigido por un supervisor, Director o el personal de los servicios de emergencia o por la ruta más directa. NO CORRA.

(4) Proseguir a la zona de evacuación de concentración designadas u otra área designada en su caso, o dirigida por un supervisor, el personal de guardia o de Servicios de Emergencia.

(5) Obedezca todas las instrucciones de un supervisor, Delegado o de personal de emergencia.

(6) No intente volver a entrar al edificio hasta que se le indique por un Director o personal de Servicios de Emergencia.

NOTA: En la medida de lo posible, y para la gestión de evacuación, seguridad y salud, todas las personas evacuadas de la construcción se mantendrán en su zona de evacuación designada hasta que la situación se estabilice.

2. Deterioro de la movilidad u otras personas con discapacidades durante una evacuación

Las personas que sufren una deficiencia de movilidad u otros perjuicios que tendría un impacto, o podría, posiblemente, el impacto, en su evacuación segura y rápida tienen una obligación legal de comunicar la naturaleza de la discapacidad al Guardián o su supervisor antes de cualquier evento que pueda requerir la evacuación. El Guardián debe discutir con la persona en cuestión los procedimientos que deben adoptarse en caso de que estén presentes durante una evacuación. Si la situación lo amerita, la discusión debe incluir el Jefe del Departamento de Salud o el lugar de trabajo y responsable de seguridad, o cualquier combinación de éstos que pueda efectuar una resolución aceptable. En cualquier caso, la persona afectada debe ser consciente de la necesidad de evacuar, por cualquier medio razonable y eficaz.

Las medidas adoptadas para evacuar a una persona afectada se espera que dependa de la naturaleza de la discapacidad y las circunstancias de la emergencia o evacuación. Puede que necesite ayuda en la localización y el uso de las salidas normales o de emergencia puede restringir o negar la posibilidad de utilizar una salida adecuada.

Cuando el deterioro de un individuo sólo en parte afecta a su capacidad para responder a una evacuación (por ejemplo, problemas de visión o la necesidad de usar las muletas) y su supervisor es consciente de la situación, una persona sana debe ser nominada para orientar o ayudar individualmente a las personas discapacitadas a la evacuación de salida y área de reunión. Si los que tienen autoridad no son conscientes, que debe ser notificada inmediatamente, o en su defecto la capacidad para hacerlo, una persona sana debe ayudar a la persona afectada. La evacuación de este individuo no debe obstaculizar el paso de la demás personas sin discapacidad.

NOTA: Una Evacuación sólo debe considerarse si existe un peligro inminente, y si otras opciones no están disponibles. Este método debe ser realizado por personal debidamente capacitado.

3. Negativa a cumplir las órdenes del delegado

Todas las personas en el lugar de trabajo en Israriego deben obedecer las instrucciones dadas por un Delegado durante una evacuación o en el ejercicio de sus funciones. De lo contrario, es un delito grave, y una vez que una persona ha sido claramente advertida de que están obligados a evacuar el lugar, la negativa debe ser reportada al Gerente o Jefe de área, que asesorará a la Oficial a Cargo de los Servicios de Emergencia. El Oficial a su discreción, puede tomar las medidas apropiadas en virtud del derecho a expulsar a la persona. (Los Servicios de Emergencia del personal son jurídicamente capaces de utilizar todos los medios que fuesen razonables y necesarios con el fin de garantizar la seguridad de todas las personas durante una emergencia o

evacuación.) El oficial encargado puede presentar cargos por el incumplimiento de la ley. Del mismo modo, el delito debe ser comunicado al Director o Gerente, que podrá someter la cuestión a los procedimientos disciplinarios.

4. Medios de comunicación

Los funcionarios no deben hablar de una emergencia o de evacuación con los medios de comunicación. Todas las solicitudes deberán ser remitidas al Gerente General, para garantizar que la información exacta no es precipitada o manipulada.

5. Simulacros de evacuación

Los Simulacros de evacuación serán determinados por el Gerente General y será quien determinará la frecuencia. Son parte integral de la seguridad de todas las personas en el lugar de trabajo, proporcionando la práctica de los procedimientos de emergencia para todos los involucrados, (lo que reduce la inseguridad durante una evacuación "real"), y también permite la determinación de las fallas en los sistemas o procedimientos, que pueden remediarse. Los Simulacros se programarán previa consulta con el Delegado de la unidad, porque normalmente no hay otras personas que tienen este conocimiento. Las reglas, responsabilidades y atribuciones de la autoridad son los mismos que para cualquier emergencia o evacuación. Por lo tanto cada situación de emergencia o evacuación deben ser tratados con el mismo sentido.

Fuego – Incendio

Si se descubre un incendio, hay tres consideraciones principales: dar la alarma, la lucha contra el fuego y la evacuación del edificio. La prioridad de estos serán determinados por las circunstancias, pero la seguridad personal es primordial en todo momento. El procedimiento de la empresa se respetará en todos los sentidos.

Al descubrir un incendio:

(1) Si la alarma no se activa automáticamente, habrá intento de activar manualmente mediante un punto de rotura de cristales.

(2) Alertar a las personas que estén cerca y obtener ayuda.

(3) Trate de apagar el fuego sólo si está familiarizado con el uso de los extintores, según el tipo de situación y si el fuego es pequeño. No entre en un espacio reducido para luchar contra el fuego, y no dejar que el fuego se interponga entre usted y la salida. Si el calor o el humo se han convertido en amenaza, salga inmediatamente y cierre las ventanas y las puertas si es seguro hacerlo.

(4) A menos que su integridad física esté comprometida en una situación de fuego, o que su ayuda sea solicitada por un Delegado usted debe evacuar el edificio inmediatamente.

(5) Seguir el procedimiento de evacuación de la manera más completa y rápida posible.

(6) Obedezca todas las instrucciones de las personas autorizadas, y no trate de entrar o volver a entrar en el edificio hasta que se el permiso sea emitido por un Delegado.

La prevención de incendios es tan importante como los procedimientos de emergencia. El personal debe asegurar que los materiales inflamables no se acumulen innecesariamente o de alguna manera o en un área en la que puede ser encendida. Los materiales deben ser almacenados de manera adecuada y no como un obstáculo para el movimiento. Corredores, escaleras, pasillos, otras formas de acceso y salidas de emergencia no deben ser bloqueado en ningún momento.

Amenaza de bomba

Hasta que se demuestre lo contrario, todas las amenazas de bomba deben ser tratadas como reales. Durante las horas de trabajo del Delegado de Unidad, este es responsable de evaluar la amenaza y la coordinar la respuesta.

Cada miembro del personal debe tener una copia de la "Lista en Amenaza de bomba", mantenerse cerca de su teléfono.

Si recibe una llamada de amenaza de bomba:

(1) Mantenga la calma, y lo más importante, no cuelgue, incluso si la llamada termina.

(2) Alerte a las personas cercanas y obtenga ayuda. No propague el rumor ya que puede causar pánico.

(3) Trate de mantener en la línea a la persona que llama a alertar, y siga la “Lista en Amenaza de bomba" si es posible.

(4) Al término de la llamada intente registrar la mayor información posible sobre la persona que usted estaba escuchando. Las señales en la parte posterior de la lista de verificación le ayudarán.

(5) Seguir las instrucciones dadas por el Delegado/Encargado o el personal de Servicios de Emergencia.

(6) En caso de que una evacuación se señale, siga el procedimiento de evacuación de la manera más completa y rápida posible. No cierre las ventanas y puertas.

Si en algún momento se descubre un objeto sospechoso, no trate de manejar la situación. Póngase en contacto con el Delegado de unidad o el segundo Encargado y siga todas las instrucciones que este le informe.

6. Explosión

La seguridad personal es de suma importancia. El procedimiento de la compañía debe ser ejecutado.

En el caso de una explosión repentina:

(1) Mantenga la calma en la medida de lo posible y tranquilice a las personas que estén a su alrededor.

(2) Evalúe la seguridad del área en la que se encuentra, tome nota de la posición de cables eléctricos, vidrios o materiales rotos, materiales colgantes, derrame de material inflamable, liberación de material tóxico o gases inflamables, No intente mover los materiales o personas a menos que sea seguro para ambos.

(3) Reporte la explosión al servicio de emergencia apropiado.

(4) Si las alarmas no se han generado automáticamente intente activar la alarma manualmente rompiendo los vidrios de la alarma.

(5) No intente extinguir el incendio a menos que este sea de proporciones menores y que usted sepa utilizar un extinguidor o que esté en inminente peligro su vida. Si es seguro siga el procedimiento de evacuación tan rápido y complete como sea posible, o evacúe por la ruta más segura disponible para usted. No cierre puertas o ventanas al salir. Si está en capacidad de atención a las personas heridas.

(6) Obedezca todas las instrucciones o direcciones dadas por el Director o personal autorizado.

(7) No intente entrar o reingresar al edificio hasta que se haya emitido orden de hacerlo por el personal a cargo.

7. Materiales peligrosos

En el caso de fugas o derrame de material peligroso:

(1) Si fuese seguro hacerlo, identifique el material dañino con el fin de emitir una respuesta correcta.

(2) Notifique al Jefe de Piso o su delegado e informe la ubicación, y si conoce la identidad del material peligroso. Suministrar toda la información posible y seguir todas las instrucciones que se le den.

(3) Evacúe el área afectada siguiendo el procedimiento tan completo y pronto como sea posible. Asistir a los incapacitados en la medida de sus capacidades.

(4) No comer o fumar hasta que el lugar sea descontaminado, o hasta que le sea permitido u ordenado por el personal de emergencia de la unidad.

(5) De ser necesario suministre primeros auxilios de acuerdo a sus conocimientos.

(6) No entre o reingrese al área afectada por el derrame o fuga hasta que esté autorizado a hacer lo por un delegado.

8. Emergencia Médica

Al encontrase con una emergencia médica:

(1) Evalúe rápidamente la situación de peligro para sí mismo y otros.

(2) Evaluar la condición de las personas. Compruebe que la persona involucrada responde a preguntas, agítela suavemente si parece inconsciente.

(3) Alerte a las personas cercanas y tome en cuenta su ayuda.

(4) Si usted piensa que la situación puede ser potencialmente mortal o existe alguna duda solicite inmediatamente una ambulancia. Siga todas las instrucciones que le den.

(5) Contactar con el jefe de vigilancia o Delegado, si están presentes, e informe de la situación. Se le notificará al funcionario más cercano de primeros auxilios, y se arreglará para que alguien solicite una ambulancia. Si no están en el edificio, designar a alguien para cumplir con este papel.

(6) Administrar los primeros auxilios según el nivel de su formación.

Terremoto

En el caso de un terremoto:

(1) No trate de salir del edificio durante el terremoto debido a los peligros de caída de materiales. Manténgase de pie en una puerta o debajo de un escritorio hasta que la situación se haya estabilizado.

(2) Evaluar la seguridad del área alrededor, tomando nota de los cables eléctricos, vidrios rotos o materiales, los materiales colgantes, derrame de

materiales inflamables / corrosivos, la liberación de materiales peligrosos o gases inflamables o tóxicos. No trate de mover los materiales o personas a menos que sea seguro para los dos.

(3) Seguir el procedimiento de evacuación lo más completa y rápida posible, manténgase alejado de los árboles, edificios y líneas eléctricas y otros materiales potencialmente peligrosos. Ayudar a otras personas en la medida de lo posible.

(4) Ser conscientes de la posibilidad que las réplicas ocurren. No entrar o volver a entrar en un edificio hasta recibir la autorización para hacerlo de un Delegado.

(5) Obedezca todas las instrucciones de Delegados y personal de Servicios de Emergencia.

(6) Si es necesario, administrar los primeros auxilios hasta el nivel de su formación.

Armas de propiedad de la compañía

Israriego Cía. Ltda. no tolera la presencia de armas en la propiedad de la compañía. Cualquier elemento que entra en la definición de un arma en la sección 5 de la Ley de Armas de 1990 se considera un arma. La presencia de un arma en la propiedad de la compañía debe ser reportada inmediatamente a su gerente. La posesión de cualquier arma en la propiedad de la compañía será tratada a través de los procedimientos disciplinarios.

Intrusos armados en propiedad de la compañía

La seguridad personal es de suma importancia. En el caso de un intruso armado en las oficinas de Israriego:

(1) No activar las alarmas de evacuar a las personas ya que el sonido puede agitar el intruso.

(2) Notificar al jefe de vigilancia o delegado si está presente en el edificio y obedecer todas las instrucciones que le dan. El Delegado tiene la responsabilidad de determinar si debe evacuar y la forma en que debe hacerlo, o aconsejar a la gente encerrarse en sus oficinas o área de seguridad.

(3) Notificar a la policía. Obedecer todas las instrucciones que le dan.

(4) Mantenga la calma y evitar la confrontación con el intruso. No enemistarse con ellos.

(5) Quédese donde está evacuado, o en su oficina, hasta que le sea indicado lo contrario por un delegado. No entrar en el edificio a menos que reciba la autorización por un Director o personal de Servicios de emergencia.

Disturbios e intrusión Pública

En cualquier situación de desorden civil o la intrusión pública en propiedad de la compañía, notifique inmediatamente a la policía, dando la ubicación y naturaleza del evento. Obedecer todas las instrucciones que le dan. Si es seguro hacerlo, restringir el acceso al edificio, y en función de los registros de eventos seguros. Mantenga la calma y evite la confrontación con los involucrados en la incursión, encerrarse en su oficina o un área segura hasta recibir la autorización de un Delegado. ¿Tienes una ruta de escape en la mente?, Utilícela solo si es necesario.

En el caso de una muerte o una lesión grave:

El jefe del departamento debe:

1. Asegurar que los familiares sean notificados por la persona adecuada (caso de que la policía está involucrada, se pondrá en contacto con los familiares.) Teniendo cuidado de garantizar que sólo se produzca una notificación;

2. Notificar a los empleados del área de trabajo;

3. Organizar un apoyo apropiado de post-trauma.

El Director Gerente debe:

(1) Gestionar todas las consultas afuera sobre el incidente, incluyendo los de los medios de comunicación.

(2) Organizar una carta de condolencia.

(3) Organizar un apropiado apoyo post-trauma

Indemnización

Delegados son indemnizados por Israriego en materia de procedimiento legal que surja como resultado de una acción realizada de buena fe en el ejercicio de sus funciones como guardián durante la operación de los procedimientos de emergencia, incluidos los de emergencia o simulacro de evacuación de un edificio.

ANEXO 3

TAREAS DEL EQUIPO DE RESPUESTA A EMERGENCIA

ÁREA DE DELEGADOS

Lista de verificación de emergencia

1. Usar un sombrero color amarillo

2. Ingresar en cada cuarto accesible e informar a los ocupantes que abandonen el edificio por las escaleras o salidas mas cercanas. Todas las puertas deben estar cerradas excepto durante una amenaza de bomba.

3. Seguir las instrucciones de los jefes de vigilancia o delegados de unidad.

No abrir las puertas con cerraduras calientes o si sale humo debajo de la puerta.

Si el área está llena de humo gatear por el piso hasta un área segura.

Responsabilidades de emergencia

En caso de emergencia, el deber principal del Guardián o Delegado de área es asegurar que todo el personal es evacuado de su piso.

Asegurarse de que cada habitación ha sido inspeccionada y que los ocupantes se han evacuado el edificio, cerrando las puertas a su paso. Revisar los baños. Lo adecuado en habitaciones cerradas es Golpear la puerta con fuerza. Si existe sospecha que hay alguien en una habitación cerrada con llave, informar al jefe de vigilancia. Tomar nota de cualquier persona que se niegue a salir

cuando se lo solicite, e informar a la jefe de vigilancia. El jefe de vigilancia puede informar a los bomberos que todavía estén en el edificio.

Asegurar que el desalojo es de manera ordenada. Llamar la atención a las personas que lleven objetos al bajar escaleras.

Cualquier persona en silla de ruedas debe ser trasladada al área de seguridad contra incendios, y luego esperar hasta que el Cuerpo de Bomberos pueda llevarlo hacia planta baja o un área segura. Asegurarse de que alguien se quede esperando con ellos.

Pedir ayuda de primeros auxilios para cualquier personal herido. Si no hay ningún oficial de primeros auxilios a la mano, entrar en contacto con el jefe de vigilancia. Realizar arreglos para que el personal herido sea trasladado a una zona aislada de fuego hasta la evacuación del edificio.

Informar sobre la evacuación del área a Jefe de vigilancia o Delegado y esperar instrucciones del mismo. Esto debe ser realizado en persona en el punto de emergencia del lugar de evacuación.

Un deber secundario es el de coordinar un ataque contra el fuego, sólo si este puede realizarse bajo niveles de seguridad. Los Guardianes o delegados, u otros miembros del personal, deben tener una formación en el uso de extintores de incendios.

Responsabilidades no de emergencia

Los guardias o delegados de área deben ejecutar el plan para evacuar de la mejor manera. Las principales consideraciones son las siguientes:

- Decidir las vías de evacuación. Lo mejor es empezar en lugares obvios de salida.

- Para evitar confusiones en caso de emergencia, sólo un director de cada área debe dar informes de evacuación al Guardia o delegado del área. Así que los guardianes o delegados deberán esperar a que cada director termine su informe.

Los Vigilantes o Delegados deben determinar si hay áreas que no deben ser comprobar en una emergencia. También, los vigilantes deben asegurarse de que tienen acceso a todas las áreas que deban revisarse.

Adicionalmente los vigilantes deben estar familiarizados con las áreas de evacuación, revisar regularmente los extintores, reportar problemas al Delegado de área en particular:

- Cualquier obstrucción en las vías de salida o evacuación.
- Ubicación de mercancías peligrosas o equipos.
- Revisar defectos en extintores o equipos de seguridad.
- Revisar señales de salida y luces de emergencia
- Esté al tanto de las personas con limitada movilidad.

Por último, los guardianes deben verificar que los procedimientos de emergencia se comuniquen al personal de su área.

Responsabilidades especiales de vigilantes

Los Guardianes deben realizar las siguientes tareas:

En momentos de emergencia:

- Evitar que vehículos ingresen en el parqueadero.

- Disuadir a las personas de entrar en el edificio.

- Verificar que la zona de montaje sea ocupada de una manera ordenada, cuidando que queden libres los lugares para vehículos de emergencia.

- Usar un megáfono y llevar el chaleco naranja de alta visibilidad en momento de emergencia.

- Los sombreros, megáfono y chalecos para guardias de servicio especial se almacenan en la bodega en el edificio administrativo.

Personal de primeros auxilios

Al oír la señal de emergencia el personal de primeros auxilios, que no beben ser los que realizan deberes de vigilancia, deben estar preparados para atender cualquier herido. Antes de proceder a la zona de emergencia, deben ir al lugar de encuentro y ayudar al jefe de vigilancia según sea necesario.

Jefe de Delegados

Responsabilidades de emergencia

1. Usar un sombrero color blanco.

2. Dirigirse al Punto de Control de Emergencias.

3. Comprobar con los Bomberos cual es la ubicación de la alarma y esperar que los bomberos determinen la causa de la alarma.

4. Establecer contacto con quienes tienen la responsabilidad de mantenimiento para el control de los servicios (gas, agua y electricidad).

5. Recibir informes de los Vigilantes de zona sobre el estado de la evacuación de sus áreas de responsabilidad. Mantener un registro escrito de esos informes.

6. Acudir al personal de primeros auxilios para atender a lesionados.

7. Supervisar que los vigilantes de área: permanezcan en el punto de control, o dirijan al personal que no ha sido evacuado al punto de reunión.

8. Mantener el control sobre los procedimientos de evacuación hasta su relevo por los Servicios de Emergencia.

9. Asesorar a los Servicios de Emergencia del estado de la evacuación del edificio, y servir de enlace con el oficial hasta la finalización de la emergencia.

10. Durante la emergencia: Informar a los ocupantes del edificio en el punto de reunión para volver a la construcción.

Prepare un breve informe escrito para entregar a los directivos de la empresa. Convocar a una reunión informativa al personal pertinente del Grupo de Emergencias del Edificio para evaluar y mejorar el procedimiento.

Responsabilidades no de Emergencia

1. Establecer y actualizar el plan de emergencia, incluido el presente Manual de Procedimientos de Emergencia.

2. Mantener actualizada la información de emergencia, incluyendo un registro de mercancías peligrosas y el equipo en el edificio.

3. Determinar la estructura adecuada para el Equipo de Respuesta de Emergencia, nombrar a todos los miembros, y organizar los reemplazos en casos de cambios. Mantener un registro de los actuales miembros del Equipo de Respuesta de Emergencia. Entrenar a nuevos miembros del Equipo de Respuesta de Emergencia en cuanto sean designados.

4. Informar sobre los obstáculos a los pasillos, pasadizos, escaleras y salidas de emergencia, y corregir el problema.

5. Fijar tiempos y fechas de al menos un simulacro de evacuación de emergencia por año.

6. Preparar y montar avisos con respecto a los procedimientos de evacuación y los deberes del personal en caso de una emergencia, en consulta con el directorio de la empresa. Estas deben incluir un plano de la unidad, en el cual se visualicen rutas de evacuación, las órdenes principales de incendios, e identificar a los Vigilantes de Área.

7. Determinar las rutas de evacuación más adecuada para la unidad y asegurar que los Vigilantes de área indicarán esto al personal. Determinar la ubicación del punto de la Asamblea.

Preparar el plan de evacuación, incluyendo la provisión para disuadir a las personas de entrar en el edificio después de la alarma.

ANEXO 4

Plan del Centro de Operaciones de Emergencia

Versión 1.0 del:

Es aprobado por

_____

Gerente General

_____

Coordinador BCP

Guía rápida de referencia

I. Activación del EOC

El EOC es activado por el Equipo de respuesta a incidentes.

II. Niveles de Activación / Personal

Nivel 1 El incidente es probable que impacte en cierto número de funciones críticas, y un posible uso del Equipo de respuesta a incidentes.

Personal: Gerente de EOC
Personal del EOC en estado de alerta.

Nivel 2 El incidente es probable que impacte a un moderado número de funciones críticas y un limitado uso del equipo de respuesta a incidentes.

Personal: Gerente de EOC
Miembros del personal de EOC

Usuarios: Miembros del equipo de respuesta a incidentes

Nivel 3 El incidente es probable que impacte a un extenso número de funciones críticas y la total activación del equipo de respuesta a incidentes.

Personal: EOC Manager
Miembros del personal de EOC

Usuarios: Equipo completo de respuesta a incidentes
Todo el equipo de respuesta táctica.

El principal EOC está ubicado en Carapungo. Si el área de la emergencia incluye el EOC primario, el EOC secundario es Quito. La persona encargada

de la activación del EOC confirma la ubicación con el personal del EOC al efectuarse la notificación.

En el caso de un evento en el sitio Carapungo el principal lugar EOC es en Oficinas Quito, situada en Av. Prensa N50-41 y Manuel Valdiviezo.

El miembro del personal EOC que se encuentra actualmente "en la llamada" informará inmediatamente a la EOC.

A su llegada al EOC se llamará al personal faltante del EOC. El esfuerzo de las comunicaciones iniciales requiere más de un miembro del personal del EOC.

Cuando el miembro del servicio EOC llega al EOC llamará a la página oficial de activación para informar que el EOC está en funcionamiento. La persona que realice la activación proporcionará al personal del EOC información sobre a quién llamar y qué mensaje proporcionar.

III. Funciones EOC

A. Proveer un Punto central del contacto

El personal de apoyo EOC realiza el papel de un centro de respuesta de emergencia y de recuperación de información. Los principales contactos telefónicos de EOC (XXXXXX) son entregados a gerencia general. Coordinador BCP y todos los jefes de equipo de IRT, TERT, y otros jefes de equipo (si es necesario)

Ellos llamaran para reportar lesiones, para actualizar el progreso en el área, encontrar algún gerente en específico, para responder preguntas de los medios.

Todo lo que ocurra dentro de las operaciones de Respuesta y recuperación eventualmente se graba en el EOC

B. Notificación Inicial

El personal del EOC es responsable de notificar a los líderes y miembros de equipo así como al gerente de EOC.

La notificación inicial deberá ser grabada en la Lista de verificación de notificaciones. Coloque el código correcto del estado del contacto y la hora de cuando la llamada fue realizada en las columnas de estado y tiempo de llamado respectivamente.

Hacer espacio para múltiples entradas, si la llamada inicial no tuvo éxito. Cada llamada requiere una hora y el estado de entrada.

C. Registro de entrada/salida de llamadas

Todas las llamadas se registran en las hojas de registro telefónico. Coloque las iniciales en la final de la entrada de registro.

D. Reunir información crítica

Los informes se publicarán en los tablones de anuncios. Otra información clave se escribirá en los tablones de presentación o papelógrafos. Mantener el sistema de seguimiento de la información actualizada al día.

E. Requerimiento de recursos.

Se llevará un registro de las solicitudes de recursos según su orden de llegada. Esa información es publicada en los indicadores de problemas sin resolver, El Administrador EOC o su suplente revisarán las solicitudes criticas de inmediato.

F. Informar a los gerentes del estado

Monitoreo del cambio de estados de emergencia y publicar la información en el cuadro de repuesta / recuperación.

El Administrador EOC o su suplente informarán al jefe de Equipo de respuesta a incidentes críticos en cuanto el EOC lo reciba.

El jefe de respuesta a incidentes podrá requerir que el personal de EOC contacte personal específico y proporcione información crítica.

G. Contactar a Gerentes para Información.

El Administrador de EOC puede requerir información de individuos específicos. El personal del EOC se localice a la persona y obtener la información necesaria. Anote la solicitud y la respuesta en el registro del teléfono. Publicar o actualizar la información sobre el adecuado estado de las juntas resuelve problemas.

H. Preguntas de medios de comunicación.

Todos los empleados tienen instrucciones de re-direccionar las solicitudes o preguntas de los medios de información al EOC. Deberá existir funcionarios designados de la empresa para ser el Oficial de Información Pública son los únicos empleados autorizados a hacer declaraciones a los medios de comunicación. Consulte todas las solicitudes al administrador de EOC.

I. Registro de operaciones de EOC

El registro de operaciones del EOC es el registro de todas las actividades realizadas por el EOC.

LISTA DE CONTACTOS

I. Personal de EOC (con Lideres del equipo de respuesta a incidentes)

Gerente de EOC

- Nombre:
- Teléfono Oficina:
- Dirección:
- Teléfono Casa:
- Otro teléfono:

Gerente de EOC alternativo

- Nombre:
- Teléfono Celular:
- Dirección:
- Teléfono Casa:
- Otro teléfono:

Líder del equipo de respuesta a incidentes

- Nombre:
- Teléfono Oficina:
- Dirección:
- Teléfono Casa:
- Otro teléfono:

Líder del equipo de respuesta a incidentes alternativo

- Nombre:
- Teléfono Oficina:

- Dirección:
- Teléfono Casa:
- Otro teléfono:

II. Líderes del equipo de respuesta a incidentes y suplentes

Información de contacto para líderes de equipo de respuesta a incidentes y equipo suplementario para todos los equipos de respuesta a incidentes.

Cargo	Nombre	Alterno

III. Miembros del equipo de respuesta a incidentes

Nombre	Numero celular	Numero Oficina	Emails

Organización del EOC

El EOC está establecido con las siguientes áreas funcionales:

- Cuarto de comunicaciones
- Sala de reuniones
- Sala de reunión de medios de comunicación
- Espacio de trabajo para los representantes del equipo.

I. Sala de comunicaciones

Incluye un único teléfono, líneas telefónicas dedicadas y un TV para controlar la prensa local. La sala está preparada para evitar que el sonido de los dispositivos de control interfirieran con las comunicaciones telefónicas. La habitación está separada de otras áreas funcionales para evitar que otras personas interfieran en el área.

II. Sala de reuniones

Suficientemente grande como para albergar cómodamente el número máximo de participantes que se esperen en una reunión. Ese número puede incluir el personal de EOC (con los líderes del Equipo de Respuesta de Incidentes y representantes de organismos externos. La sala de reuniones debe estar equipada con el panel de estado, carteleras y pizarras, (sólo se usan pizarras movibles como respaldo de seguridad si es posible) para el seguimiento del proceso de recuperación el EOC debe actualizar el panel de estado. El espacio y las conexiones estarán disponibles para un televisor si las conferencias de prensa televisada a partir de otras fuentes puede ser una parte de las reuniones

III. Sala de comunicaciones a medios

No debe estar dentro del perímetro de seguridad del lugar de reunión del EOC. La sala de comunicaciones a medios es una sala de acceso controlado para asegurar que sólo los miembros de la prensa/medios tienen acceso. La habitación estará configurada para soportar sesiones de información para los medios de comunicación. Se designará espacios de estacionamiento para el los transportes de satélite de enlace.

IV. Lugar de trabaja de respuesta a incidentes

Disponibles para los representantes del equipo co-ubicado en el COE. Cada espacio incluye líneas de voz, datos y de alimentación de energía. Un UPS y un generador para suministrar energía en caso de interrupciones del servicio de energía del COE.

Suministros y Equipos de EOC

I. Comunicaciones

- Teléfonos
- Fax and back up de fax
- Línea telefónica Dedicada (no conectada a central telefónica)
- Teléfonos celulares con cargadores que permiten carga hablar durante las operaciones.
- *Radios. (WalkieTalkie) según sea necesario.*
- *Televisión, vídeo, radio AM / FM*

II. Suministros de oficina

- Block de hojas
- Post it
- Lápices
- Sacapuntas
- Marcadores y borradores para pizarras blancas
- Cintas de vídeo en blanco
- Cinta adhesiva
- Linternas y pilas de repuesto
- Impresora / copiadora de papel
- Un marco de caballetes con blocs de papel blanco (para aumentar las pizarras blancas)
- Carpetas de archivo, clips, gomas, tijeras, grapadoras, etc

III. Equipos de oficina

- PC's
- Impresoras (2 o mas)
- Copiadoras (2)

- Trituradora de papel
- Perforadora
- Grabadora

IV. Documentos

Plan de Continuidad de Negocios

- Rol de Pagos y beneficios
- Building Blueprints (All buildings)
- Mapa de red eléctrica
- Local Street guide/map
- Directorio Telefónico
- Listado de contacto de sucursales

Información detallada

I. Activación del EOC

CUANDO

El EOC es activado por orden de **XXXXX.**

La notificación de activación será realizada por **XXXXX** u otro funcionario designado como tal.

DONDE

El EOC primario está localizado en las Oficinas de **Carapungo**. SI el área de emergencia está localizada en el EOC primario, el EOC secundario es en las oficinas de **Quito** y operará como principal.

Si la ubicación primaria y secundaria fuesen afectadas, el personal a cargo del ECO decidirá la ubicación a utilizarse y deberá ser oficialmente notificada.

QUIEN

El miembro del personal del EOC que se encuentra actualmente "en la llamada" deberá reportar inmediatamente un informe al EOC.

Esta persona debe llamar al personal de apoyo del EOC. El esfuerzo de las comunicaciones iniciales requiere más de un miembro del personal del EOC.

EL EOC será gerenciado por **XXXXX.**

El personal de soporte "En la llamada" será **XXXXX.**

El apoyo del EOC del día a día serán manejados por contribución de **XXXXX**.

QUE

Cuando los miembros del EOC lleguen al lugar de encuentro, la responsabilidad de el/ella será realizar la llamada o informar que la activación del ECO es oficial y está en funcionamiento.

El funcionario que realice la activación del EOC puede llamar a otros miembros del personal si el teléfono del personal primero en la lista esta ocupado. El personal de guardia debe registrar esto.

El funcionario de la activación proporcionará al personal EOC con información sobre a quién llamar y qué mensaje que dar.

DETALLE DE FUNCIONES EOC

I. Proporcionar un punto central de contacto

El personal de apoyo EOC actúa como un centro de respuesta y recuperación de información. Como tal, el EOC ofrece un servicio crítico en los momentos difíciles. El principal número de teléfono entrante EOC (s) es **XXXXXXXXXXX**, se le dará a todos los miembros del Equipo de Respuesta / Recuperación.

Llamar para reportar los lesionados; para actualizar los avances en su área, para ubicar a un administrador específico, para asesorarse sobre preguntas de los medios, etc. Todo lo que sucede durante las operaciones de respuesta / recuperación con el tiempo se registrarán en la EOC.

Otras funciones de EOC son:

- Realizar la notificación Inicial
- Realizar registro de Entrada / Salida llamadas
- Reunir información crítica
- Recibir las solicitudes de recursos
- Informar a los gerentes clave del estado de
- Gestionar Contactos para Información
- Recibir preguntas de los medios (Directo al Oficial de Información Pública)

II. La notificación inicial.

Después de la activación oficial notificar al personal de guardia EOC, él / ella debe iniciar el proceso de notificar a los directivos clave de la situación. Cuando el personal del EOC activa el EOC, el personal del EOC debe asumir la responsabilidad de notificar a los administradores de otras áreas. El funcionario de la activación debe proporcionar al personal EOC el mensaje que se dará a los gerentes clave. Él / ella también le dirá al personal de EOC a

quién contactar. El personal de estos centros apuntarán el mensaje y a quién contactar palabra por palabra. El miembro del personal de estos centros debe leer el mensaje de nuevo al oficial de la activación para asegurar que la información es correcta. Si el funcionario o el personal de la activación de EOC recibe un contestador automático, dar un breve mensaje explicando la situación y pedir que llamen al EOC para más información.

NO REALIZAR LLAMADAS DESDE EL TELÉFONO DE EMERGENCIAS(S) este es solo para las llamadas entrantes (XXXXXXXXXXX).

El funcionario de la activación deberá dar un informe al EOC, tan pronto como sea posible después de la activación. Al llegar, el oficial de la activación se hará cargo de las funciones de la EOC. Registrar la notificación inicial en la lista de control de notificación. Colocar el código de contacto y el momento en que se hizo el llamado. Hacer espacio para múltiples entradas, si la llamada inicial no es un "contacto con éxito". Cada llamada requiere una entrada de tiempo y el estado.

III. Registro de llamadas entrantes / salientes

Registrar todas las llamadas en las hojas de registro de teléfonos. La siguiente información es requerida como obligatorio en todas las llamadas internas y externas:

- Fecha y hora de la llamada
- Nombre de la persona que se llama

Para las llamadas entrantes también incluyen las medidas adoptadas por el miembro del personal EOC en relación a la llamada. Algunos ejemplos incluyen:

- "Aprobado por la información de (nombre)"
- "Respuestas a _____" persona que llama pregunta sobre

Las iniciales de la persona que maneja la llamada debe estar al final de la entrada del registro.

¿Por qué mantener los registros de TELEFONÍA?

Las situaciones de emergencia o un desastre pueden ser confusas. Mucha de la información transmitida por teléfono es fundamental para la recuperación. Información importante podría perderse a menos que todas las llamadas telefónicas sean grabadas con precisión.

Después de una emergencia es importante para estudiar las medidas adoptadas por todos los participantes. Podemos identificar lo que hicimos bien y qué necesita ser mejorado. La mayoría de las acciones tomadas en caso de emergencia son por teléfono. Es difícil de estudiar nuestras respuestas, sin un registro preciso de las acciones telefónicas.

IV. Reunir información crítica

Información precisa y oportuna es esencial para una respuesta eficaz a la emergencia y recuperación de desastres. El EOC es un centro de información sobre:

- ¿Cuáles son los problemas no resueltos?
- ¿Lo que se necesita y donde se necesita?
- ¿Cómo lo estamos haciendo?
- ¿Quién está trabajando, en qué, y dónde están?

Los departamentos en los informes diarios que proporcionan la mayor parte de esta información. Parte de la información se proporcionará a través del

teléfono. Habrá un sistema establecido para el seguimiento de esta información. Los informes se publicarán en los tablones de anuncios. Otra información clave se escribirá en los tablones de presentación o papelógrafos. El Administrador o Gerente EOC alternativo es responsable de establecer la información.

El personal del EOC es responsable de mantener el sistema actualizado.

Presentar el estado de las siguientes tareas sin resolver en cada área:

- Personal
- Salud y Seguridad
- Los equipos de recuperación
- Unidades de Negocio
- Operaciones Informáticas
- Operaciones de Producción
- Comunicaciones
- Equipos
- Compras
- Servicio de Ordenes de Trabajo
- Respuesta / Recuperación de la situación
- Situación de desastre (por ejemplo, crestería de los ríos, cierre de carreteras, daños en servicios públicos locales, las nevadas adicionales)

V. Las solicitudes de recursos

La recuperación de desastres requiere de muchos tipos de recursos. Estos recursos pueden incluir:

- Las personas
- Los miembros del Equipo de Respuesta de Incidentes (IRT)
- Equipo táctico de respuesta a emergencia (TERT)

- Guardias de Seguridad
- Servicio de Personal
- Los empleados temporales
- Apoyar a los proveedores
- Suministros
- Sustitución de suministros de oficina
- Suministros de recuperación
- Ordenador papel de la impresora, cintas, etc
- Salud y Seguridad
- Agua y alimentos
- Vacunas
- Reemplazo de Equipos de Producción
- Equipo de producción adicional
- Sustitución de Equipos
- Equipos adicionales
- Equipo Especial de Recuperación
- Muebles
- Sustitución
- Adicional

El personal del EOC debe registrar las solicitudes de recursos según van llegando Esa información se publicará en el adecuado estado de las juntas resuelve problemas. El Administrador o Gerente EOC alterno se ocupará de las peticiones fundamentales de inmediato.

VI. Informar a los directivos clave de la Condición Jurídica y Social

La situación puede cambiar rápidamente durante las operaciones de recuperación de un desastre. Las personas en posiciones de toma de decisiones requieren la información más reciente para que puedan tomar las mejores decisiones posibles. Los gerentes asignados para llevar a cabo la

respuesta y las tareas de recuperación deben ser informados tan pronto como sea posible de los cambios en esas tareas.

El personal del EOC hará un seguimiento de la evolución de la situación de los informes para dar una respuesta a la Junta de Recuperación de Situación. El Administrador o Gerente EOC alternativo informará al Coordinador de BCP de información crítica.

El Coordinador del BCP podrá exigir que el personal del COE contacto con personal específico y les proporcionan la información crítica.

VII. Gestores de Contactos para Información

Los líderes de Respuesta a Incidentes de equipo o jefe EOC puede requerir información de individuos específicos. El personal del COE se localice a la persona y obtener la información necesaria. Anote la solicitud y la respuesta en el registro de las llamadas ya que la mayoría se hace contacto por teléfono. Asegúrese de enviar o actualizar la información sobre el adecuado estado de las juntas resuelve problemas.

VIII. Las preguntas de los medios de comunicación

Es probable que la Prensa, radio, y los reporteros de televisión deseen información sobre la empresa y la situación de emergencia. Todos los miembros del equipo están obligados a pasar a lo largo de estas solicitudes del EOC.

XXXXXXXXXX o un funcionario de la empresa designado para ser el Oficial de Información Pública son los únicos empleados autorizados para hacer declaraciones a los medios de comunicación. Consulte todas las solicitudes de XXXXXXXXXX o el gerente encargado EOC.

IX. Registro de operaciones EOC

El Registro de Operaciones del EOC es un registro oficial de todas las actividades realizadas por el EOC. El director de EOC debe asegurar que la información a recoger sea:

- La hora y la fecha en que el EOC comienza y termina sus operaciones.
- ¿Quién está trabajando en los cambios de turno EOC, etc
- Toda la información crítica proporcionada al COE de cualquiera de los siguientes:
- Registro de Teléfonos
- Informes y reportes
- TV y Radio Conferencias de Prensa
- TV y Radio anuncios
- Copias de las proclamaciones
- Historias pertinentes de Periódico
- Informes diarios
- Registro de reunión de recuperación
- Directivas verbales y publicadas

X. Preparación para la recuperación

Los planes del equipo están destinados a ser documentos vivos. Deben reflejar la información más reciente disponible. Los líderes del BCP, el Coordinador y el equipo son responsables de revisar y actualizar sus planes en forma semestral.

El líder del equipo, líder del equipo alternativo y otras personas que tienen copias del plan de equipo deben enviar las actualizaciones cada vez que este sufra cambios. La práctica aceptada consiste en imprimir y distribuir sólo la página o páginas que han cambiado más que todo el plan.

Las portadas de las actualizaciones del plan se adjuntan al final de esta sección.

A. frecuentes Revisión del Plan

Jefe de equipo y líder del equipo alternativo:

En esta sección se identifica a las personas asignadas a los puestos de liderazgo. Que debe ser revisado por el líder del equipo para identificar los cambios en el personal asignado.

Equipo de Respuesta a Incidentes de alerta de la lista:

Esta sección proporciona información de contacto de todo el personal asignado al equipo. Esta lista es propensa a cambiar ya que los miembros del equipo pueden salir o dejar de formar parte del equipo, los nombres pueden cambiar debido a la unión y la información de contacto puede cambiar. El líder del equipo debe enviar una copia de la lista de incidentes al Equipo de Respuesta de alerta para cada miembro del equipo de revisión y actualización.

Lista de funciones críticas:

En esta sección, se encuentran en Jefe del Proyecto, se identifican las funciones básicas que se aplican al equipo. El líder del equipo de revisión de las funciones para determinar su exactitud.

Los pasos del equipo de recuperación:

Esta sección identifica las estrategias para la recuperación de las funciones críticas. El líder del equipo de revisión de esta lista para determinar que las estrategias se cumplan los objetivos de negocio actuales y reflejan con precisión la mejor solución posible.

Proveedores y listas de clientes:

En esta sección se identifica la información de contacto de proveedores clave y clientes. El líder del equipo debe revisar esta lista para determinar que la lista es completa y exacta.

Requisitos del área de trabajo:

Esta sección identifica los recursos críticos necesarios para apoyar la recuperación en el sitio de área de trabajo. El líder del equipo de revisión de esta lista para determinar que la lista es completa y exacta.

Fuera del Sitio almacenan materiales:

Esta sección identifica los registros críticos o los recursos almacenados fuera del sitio. El líder del equipo debe revisar esta lista para determinar que la lista es completa y exacta.

B. Capacitación y Ejercicios

Los planes actualizados no son suficientes si las personas asignadas a los equipos de recuperación no saben lo que se espera de ellos. Los miembros del equipo deben recibir capacitación sobre los conceptos de recuperación en general y las funciones de su equipo en particular. Los ejercicios ayudan a identificar las mejoras necesarias en las estrategias y planes. Los ejercicios también dar a los miembros del equipo una valiosa experiencia en el trato con los desafíos inherentes a las operaciones de recuperación.

Los jefes de equipo en cooperación con la formación de la conducta BCP Coordinador y ejercicios. Ejercicios propuestos son los siguientes:

Equipo de Orientación de socios:

Este es un resumen de una hora del Programa de Continuidad del Negocio. Cada miembro del equipo debe asistir una vez al año. También está disponible para la población en general del empleado.

Equipo de Ejercicio:

Todo el equipo participa en un ejercicio de simulación de dos horas con un enfoque en sus estrategias de recuperación.

Equipo de Ejercicio Líder:

Todos los jefes de equipo y líderes del equipo suplente participar en un ejercicio de simulación de dos horas con un enfoque en las instalaciones de recuperación de ancho.

El ejercicio funcional:

Manos a la real prueba de la capacidad de hardware o de conectividad en los Centros de Trabajo de recuperación de la zona. El uso real de los suplentes (manual) del proceso de producción en el hogar o centro alternativo.

C. Calendario de actividades

Este documento permite a los jefes de equipo para seguir su propio plan de actividades de revisión, la formación y el ejercicio para el año. Los líderes del BCP y el Equipo Coordinador periódicamente solicitar una copia del documento para revisar el estado del equipo de preparación. Un nuevo documento se pondrá en marcha cada año. El Coordinador del BCP se mantendrá de cada año calendario completado la actividad en el archivo para fines de auditoría.

D. Programa de actividades

Revisiones del Plan

Introduzca las fechas en que se llevaron a cabo revisiones de los planes.

Jefe de Equipo	Venc Ene1	Venc Jul 1
Lide de Equipo (Nombre):		
Jefe de Equipo Alternativo (Nombre):		
(Nombre):		
(Nombre):		

Formación / Ejercicios

Introduzca las fechas y número de participantes para cada actividad. Cada tipo de ejercicio se espera que sea llevado a cabo al menos una vez al año.

Actividad	Fecha de Actividad	# de Participantes	Comentarios
Orientación			
Equipo de Ejercicio			
Jefe de Equipo			

Líderes de Equipo: Adjuntar signo de los participantes en las hojas, las evaluaciones y los comentarios a esta hoja.

Enviar esta página al Coordinador del BCP a más tardar el 1 de diciembre.

BCP Coordinador: Guarde todos los documentos en carpetas asociadas a más tardar hasta el 15 de diciembre. Distribuir un formulario de nueva actividad a la Lista de los Jefes de Equipo, esto hasta el 01 de enero.

E. Plan de Actualizaciones

Cada vez que se actualice un plan, las hojas nuevas o modificadas se enviarán todos los titulares de planes con una portada que identifique las páginas que se sustituyen. Cada titular de plan que recibe las actualizaciones colocará la cubierta en el plan detrás de esta página.

Plan de actualización debe identificar la fecha del cambio, las páginas que deben retirarse y añadir las nuevas páginas.

ANEXO 5

PLAN GLOBAL DE GESTIÓN DE CRISIS DE ISRARIEGO

1.0 INTRODUCCIÓN

1.1 ALCANCE

Este Plan se aplica a los negocios de ISRARIEGO y a las posibles crisis que puedan afectar a la empresa. El grado de participación de ISRARIEGO en un incidente estará guiado por la posible exposición a la Empresa.

1.2 DEFINICIONES CLAVE

Las crisis se originan a partir de uno de los tres puntos iniciales. Éstos pueden describirse como incidentes asociados con un problema emergente, algún tipo de interrupción comercial o una emergencia.

Para este Plan y el proceso general de gestión de crisis, son importantes las siguientes definiciones, que se utilizarán uniformemente en todo el Plan y en toda la Empresa.

Interrupción comercial: La interrupción de un proceso comercial, producción, servicios y/o entrega al punto que dañe la estabilidad financiera del negocio o la posición en el mercado de la organización que participa en el proceso comercial.

Emergencia: Toda situación, real o inminente, que ponga en peligro la seguridad, la integridad y el bienestar de los empleados, clientes, visitantes y propiedad de ISRARIEGO, además del medioambiente.

Problemas emergentes: Un problema o una serie de incidentes aparentemente inconexos que pueden generar noticias negativas o dañar la reputación si se hacen públicos y que puedan tener como resultado multas, resarcimiento por daños y perjuicios, gastos no calculados en el presupuesto y otros costos (por ejemplo, defectos del producto, fallos de diseño, ética comercial) que superen la cantidad determinada previamente.

Incidente: Un suceso, una serie de sucesos o un conjunto de circunstancias que interrumpen los procedimientos operativos normales.

Crisis: Un suceso extraordinario que puede poner en peligro la vida de los empleados, interrumpir las operaciones o afectar gravemente la solidez financiera o la imagen pública de la Empresa.

1.3 RIESGOS Y VULNERABILIDADES

Un objetivo importante de este Plan Global de Gestión de Crisis es evitar que un incidente se convierta en una crisis, independientemente de la naturaleza del riesgo o de su ubicación geográfica. Al reconocer que los riesgos y las vulnerabilidades que enfrenta ISRARIEGO cambian constantemente, este Plan define un proceso universal que puede aplicarse a cualquier riesgo o vulnerabilidad.

El siguiente cuadro muestra los diversos tipos de incidentes que podría enfrentar ISRARIEGO. Esta lista no es exhaustiva, pero ejemplifica el alcance de aplicación del Plan:

TIPOS DE INCIDENTE CON POSIBLE CRISIS		
SEGURIDAD	**|OPERATIVO**	**AUTORIDAD CORPORATIVA**
Inestabilidad política/desorden civil	Productos/materiales peligrosos	Malversación de fondos corporativos.
Conflictos internacionales	Incendio/Explosión	Fraude/escándalo
Actos terroristas	Problemas ambientales	Malversación de fondos
Secuestros	Accidentes de transporte	**DESASTRES NATURALES**
Protestas de consumidores o activistas	Fallas de TI de gran escala	Inundaciones
Espionaje	Interrupciones en la cadena de suministros.	Tormentas
PRODUCTOS	Pérdida de servicios públicos	Terremotos
Retirada de productos	Costo/disponibilidad de energía	**RELACIONES PUBLICAS**
Problemas de seguridad y calidad	**GUBERNAMENTAL**	Problemas de la comunidad
Productos de proveedores por debajo del promedio.	Proceso de fabricación	Problemas con medios de Comunicación locales/nacionales
Conformidad de productos.	Medida normativa negativa	Violación de marcas
EMPLEADOS	Mano de obra	**FINANZAS**
Sabotaje de los empleados	Medioambiente	Disminución de la calificación crediticia
Violencia en el lugar de trabajo	Finanzas	Error en los informes financieros
Conflicto laboral	Transporte	Pérdida de inversiones
Salud y seguridad ocupacional	Incumplimiento normativo	**LEGAL**
Acoso/discrimación	Seguridad y salud	Juicios
	Barreras comercio/normas	Propiedad intelectual

2.0 ESTRUCTURA DE GESTIÓN DE CRISIS

2.1 ESTRUCTURA GENERAL DE RESPUESTA

Un gran porcentaje de todos los incidentes se manejará en el nivel de respuesta a incidentes. Sin embargo, el pequeño porcentaje restante necesitará la activación de a estructura de respuesta a la gestión de crisis y la participación de la dirección ejecutiva. La estructura de gestión de crisis en niveles que se muestra a continuación define la manera en que ISRARIEGO integrará y aumentará los esfuerzos de gestión de crisis en la Empresa.

La estructura de gestión de crisis de ISRARIEGO tiene tres niveles funcionales: respuesta a incidentes, soporte corporativo ante incidentes y gestión corporativa de crisis. Esta sección del Plan describe las funciones y las responsabilidades de los equipos en cada nivel funcional dentro de la organización.

Las actividades de respuesta a incidentes abordan las necesidades inmediatas en el lugar que surgen durante un incidente. La función principal de Respuesta a incidentes es táctica, e incluye la respuesta inicial ante emergencias y todos los requisitos de respuesta inmediata en el lugar afectado, de acuerdo con los planes, procedimientos y procesos establecidos de Respuesta a incidentes.

Soporte corporativo ante incidentes es la respuesta operativa que se lleva a cabo para proporcionar recursos corporativos adicionales y asistencia para la gestión de un incidente, en todas las áreas funcionales. Si el incidente afecta a varios sitios, divisiones o regiones geográficas, el nivel Soporte corporativo ante incidentes coordinará los esfuerzos generales de respuesta.

Gestión corporativa de crisis está compuesto por la respuesta estratégica de la Empresa a una posible crisis. Las consecuencias estratégicas y a largo plazo de un incidente son el foco principal de la función Gestión corporativa de crisis.

2.2 FUNCIONES Y RESPONSABILIDADES DE LOS EQUIPOS

Cada uno de los tres niveles funcionales arriba mencionados es implementado por un equipo de respuesta. Los tres equipos de respuesta son los siguientes:

- Equipo de Respuesta a Incidentes (IRT)
- Equipo de Soporte Corporativo ante Incidentes (CIST)
- Equipo de Gestión Corporativa de Crisis (CCMT)

2.2.1 Equipo de Respuesta a Incidentes

El Equipo de Respuesta a Incidentes (IRT) es responsable de brindar una respuesta táctica e inmediata en el lugar de los hechos ante emergencias o incidentes. Puede haber más de un equipo de respuesta a incidentes de ISRARIEGO en una unidad o en un sitio. El Equipo de Respuesta a Incidentes puede tener la forma de un equipo de respuesta ante emergencias (es decir, el equipo que responde ante emergencias de incendios, de seguridad o médicas) o de un equipo de respuesta funcional (por ejemplo, el equipo de respuesta de TI). La cantidad de miembros y la composición de los equipos de respuesta a incidentes variará según el tamaño y la complejidad de la unidad, y también según los posibles riesgos que podrían afectar a la unidad.

Las responsabilidades del Equipo de Respuesta a Incidentes son las siguientes:

- Proporcionar una respuesta inmediata ante emergencias.

- Llevar a cabo la evaluación de los incidentes y determinar los recursos que son necesarios.

- Notificar al Equipo de Soporte Corporativo ante Incidentes sobre la base de los umbrales de notificación.

- Mitigar la situación de emergencia.
- Implementar planes de continuidad comercial o de retirada de productos.
- Restaurar las operaciones normales.
- Comunicarse con las partes afectadas y necesarias.
- Coordinar las comunicaciones públicas con el Departamento de Comunicaciones Corporativas.
- Gestionar la respuesta y la recuperación en el lugar.
- Garantizar que las actividades de respuesta en el lugar sean adecuadas.

Los IRT responderán de acuerdo con los planes establecidos de respuesta ante emergencias o con los planes y procedimientos para contingencias de otras unidades que ya estén implementados. Estos planes de respuesta ante emergencias de las unidades son documentos separados que se coordinarán e integrarán con este Plan Global de Gestión de Crisis, pero que no forman parte de él.

2.2.2 Equipo de Soporte Corporativo ante Incidentes

La función de soporte ante incidentes será llevada a cabo por el Equipo de Soporte Corporativo ante Incidentes (CIST). El CIST es el equipo de nivel corporativo, responsable de garantizar que las unidades y las divisiones cuenten con los mejores recursos disponibles, necesarios para gestionar un incidente con eficacia. Luego de la activación, el CIST no sólo proporcionará el mecanismo para identificar los problemas estratégicos, sino que también actuará como un intermediario entre el equipo de nivel ejecutivo.

(Equipo de Gestión Corporativa de Crisis) y los equipos de respuesta a incidentes.

El CIST ofrece recursos, como personal, instalaciones, financiación, vehículos, equipos o suministros que no están disponibles para los equipos de respuesta a incidentes. Generalmente, el CIST opera desde una ubicación central, pero es posible que algunos miembros del CIST sean enviados a la unidad o al sitio, según la naturaleza del incidente.

Cuando un incidente afecte a varias divisiones o unidades, el CIST decidirá el orden de prioridad de las necesidades y actuará como un centro de intercambio de información para toda la información disponible relacionada con el incidente. El CIST reunirá, verificará y divulgará la información sobre el incidente, con las contribuciones realizadas por los equipos de respuesta a incidentes pertinentes.

La función del CIST es reducir las demandas de información que tienen los equipos de respuesta a incidentes que participan en la respuesta. También proporciona un mecanismo para garantizar que se comprendan los hechos comunes sobre el incidente y que todos los equipos de respuesta y la dirección de Israriego que compartan la información y las acciones de respuesta oportunamente.

Las responsabilidades del Equipo de Soporte Corporativo ante Incidentes (CIST) son:

- Brindar los mejores recursos disponibles o la pericia técnica de la Empresa al Equipo de Respuesta a Incidentes.

- Coordinar las actividades de respuesta de los departamentos funcionales.

- Brindar un centro de intercambio de información para toda la información sobre el incidente.

- Evaluar y pronosticar las consecuencias corporativas que podría tener el incidente para ISRARIEGO.

- Definir las necesidades de comunicación que se encuentren fuera del alcance del plan de comunicación de incidentes.

- Apoyar la respuesta a incidentes, incluida la retirada de productos, la continuidad comercial, la reanudación y la recuperación.

- Gestionar los problemas que excedan la autoridad del Equipo de Respuesta a Incidentes.

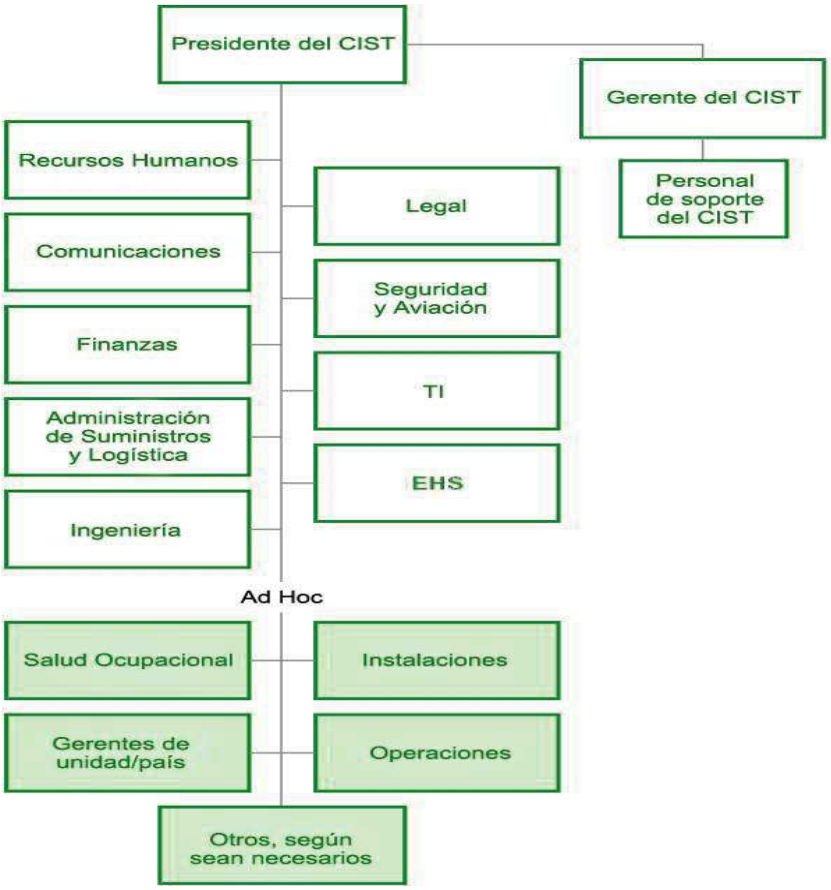
- Obtener información para los problemas planteados por la dirección ejecutiva y hacer aportes con relación a ellos.

- Identificar e intensificar los temas estratégicos con el Equipo de Gestión Corporativa de Crisis.

- Coordinar la implementación de estrategias aprobadas por el CCMT.

2.2.2.1 Pertenencia al CIST

Los miembros principales del CIST son líderes funcionales específicos dentro de la Empresa, como se muestra en el cuadro de composición del equipo. Las unidades comerciales afectadas serán presentadas ante el CIST como miembros ad hoc una vez que se active el CIST.



COMPOSICIÓN DEL EQUIPO DE SOPORTE CORPORATIVO ANTE INCIDENTES

(Las personas que actualmente trabajan en estas posiciones del CIST figuran en la Lista de funciones del CIST)

2.2.2.2 Presidente del CIST

El Presidente del CIST proporciona un liderazgo general y dirige las actividades del CIST y sus responsabilidades son:

- Evaluar el informe inicial de un incidente tras consultar con los miembros del CIST y el líder del Equipo de Respuesta a Incidentes.

- Proporcionar actualizaciones periódicas al Presidente del CCMT, según corresponda.

- Llevar a cabo reuniones y actividades del CIST.

- Actuar como punto de contacto oficial con los equipos de respuesta a incidentes y con el Equipo de Gestión Corporativa de Crisis.

- Autorizar actividades, comunicaciones y equipos de respuesta que puedan ser necesarios para brindar apoyo en el incidente o a los IRT.

- Recomendar la activación del CCMT.

- Designar a los miembros ad hoc del CIST para el incidente.

- Tomar la decisión de desactivar el CIST.

- Establecer el proceso y el cuerpo de revisión posterior al incidente una vez finalizado el incidente.

- Participar en la capacitación y en los ejercicios de gestión de crisis.

2.2.2.3 Gerente del CIST

El Gerente del CIST realiza la coordinación general de la reunión del CIST, y también su activación y el proceso de toma de decisiones.

Las tareas del Gerente del CIST son las siguientes:

- Garantizar que se contacte y se congregue a todos los miembros del CIST para la convocación o la activación.

- Asegurar que se anuncien todas las cuestiones de respuesta en el formulario de seguimiento de problemas, como fueron identificadas por el CIST durante la activación, y que se realice el seguimiento.

- Garantizar que todas las actividades y comunicaciones de gestión de crisis sean coherentes con las políticas de la Empresa y con las reglamentaciones gubernamentales.

- Asegurar que las políticas y los procedimientos del CIST estén claramente definidos y que los miembros del equipo reciban capacitación.

- Garantizar que los nuevos miembros del CIST reciban capacitación sobre las funciones y las responsabilidades del equipo.

- Llevar una lista con todos los contactos clave.

- Coordinar y divulgar el cronograma de reuniones en curso del CIST.

2.2.2.4 Miembros del CIST

Los miembros del CIST cumplen dos funciones principales: (1) como parte del equipo que toma decisiones, evalúan las consecuencias generales del incidente y (2) representan a sus respectivas áreas corporativas funcionales en respuesta al incidente.

Las tareas de los miembros del CIST son las siguientes:

- Dar prioridad a las responsabilidades del CIST de acuerdo con las responsabilidades funcionales diarias, como lo determina el Presidente del CIST.

- Familiarizarse con las funciones individuales, las responsabilidades y los procedimientos generales del CIST.

- Contribuir con la pericia y los antecedentes funcionales a los esfuerzos de respuesta.

- Llevar a cabo investigaciones, reunir información y realizar otras tareas, según las asigne el Presidente del CIST.

- Designar a un sustituto para cubrir responsabilidades funcionales de las operaciones diarias al mismo tiempo que actúan en el CIST activado.

- Participar, según corresponda, en el proceso de revisión posterior al incidente con el Presidente del CIST.

- Participar en la capacitación y en los ejercicios de gestión de crisis.

Según el tipo de incidente y a criterio del Presidente del CIST, pueden presentarse al CIST los miembros ad hoc para el período que dure el incidente.

2.2.2.5 Personal de soporte del CIST

Deben nombrarse dos o tres personas que actuarán como empleados de registro para reunir información clave durante las reuniones, asistir al Presidente del CIST, responder llamadas y tomar mensajes para los miembros del CIST. Las tareas adicionales son las siguientes:

- Tomar notas de las reuniones del CIST y publicarlas con la orientación del asesor legal.

- Documentar las decisiones y las actividades asignadas en los formularios de seguimiento de problemas y de actividades.

- Distribuir la documentación a los miembros apropiados del equipo.

- Mantener el informe de incidentes y otras herramientas de trabajo.

2.2.3 Equipo de Gestión Corporativa de Crisis

La función de gestión de crisis será llevada a cabo por el Equipo de Gestión Corporativa de Crisis (CCMT). El CCMT es el cuerpo encargado de la toma de decisiones, en el nivel ejecutivo, para responder a incidentes que amenazan con convertirse en una crisis para la Empresa. Por lo general, el CCMT participará sólo en aquellos incidentes relativamente poco frecuentes que amenazan con tener un impacto negativo sustancial e inmediato en la salud y la seguridad de ISRARIEGO, y también en el entorno, la marca, la imagen, el valor para los accionistas o la reputación de la empresa. El enfoque principal del CCMT es estratégico. El CCMT aprobará las estrategias adecuadas para ocuparse de las consecuencias corporativas y para resolver todos los problemas corporativos que surjan como resultado del incidente. Este equipo tiene autoridad para definir la política corporativa y comprometer los principales activos corporativos en respuesta a una posible crisis.

Las responsabilidades del Equipo de Gestión Corporativa de Crisis son:

- Supervisar la respuesta estratégica y las actividades de soporte.

- Tratar las consecuencias estratégicas y a largo plazo de un incidente.

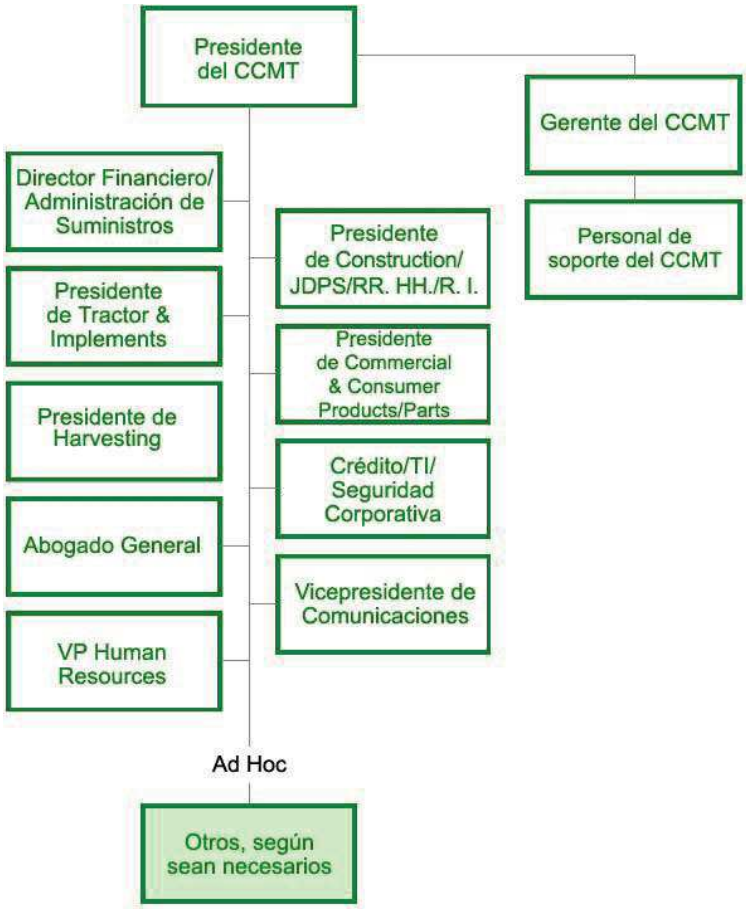
- Gestionar problemas estratégicos que excedan la autoridad del CIST y del IRT. Identificar, evaluar y gestionar aquellos problemas estratégicos que afecten ampliamente a la Empresa.

- Establecer prioridades para el desarrollo de estrategias en respuesta a posibles consecuencias específicas.

- Tomar decisiones ejecutivas para responder a crisis potenciales y reales.

- Informar al Director Ejecutivo

COMPOSICIÓN DEL EQUIPO DE GESTIÓN CORPORATIVA DE CRISIS



(Las personas que actualmente trabajan en estas posiciones del CCMT figuran en la Lista de funciones del CCMT)

2.2.3.1 Presidente del CCMT

El Presidente del CCMT proporciona liderazgo general y dirige las actividades estratégicas de gestión de crisis de ISRARIEGO. Las responsabilidades del Presidente del CCMT son:

- Evaluar los informes iniciales del incidente o de la crisis tras consultar con los miembros del CCMT.

- Tomar la decisión de activar el CCMT y nombrar a los miembros ad hoc del equipo.

- Llevar a cabo reuniones y actividades del CCMT.

- Cuando sea necesario, actuar como la persona encargada de tomar la decisión final sobre las acciones y las estrategias del CCMT.

- Autorizar las actividades o comunicaciones que no estén previstas específicamente en el Plan Global de Gestión de Crisis.

- Notificar e informar al Director Ejecutivo sobre la respuesta al incidente y sobre el estado de la gestión de la crisis.

- Nombrar a los nuevos miembros del CCMT.

- Tomar la decisión de desactivar el CCMT.

2.2.3.2 Gerente del CCMT

El Gerente del CCMT realiza la coordinación general de la reunión del CCMT, y también su activación y el proceso de toma de decisiones.

Las responsabilidades del Gerente del CCMT son:

- Asegurar que se anuncien todas las cuestiones de respuesta en el formulario de seguimiento de problemas, como fueron identificadas por el CCMT durante la activación, y que se realice el seguimiento.

- Garantizar que todas las actividades y comunicaciones de gestión de crisis sean coherentes con las políticas de la Empresa y con las reglamentaciones gubernamentales.

- Asistir al Presidente del CCMT cuando convoque al CCMT, al localizar y ponerse en contacto con los miembros del CCMT.

- Asegurar que las políticas y los procedimientos del CCMT estén claramente definidos y que los miembros del equipo reciban capacitación.

- Garantizar que los nuevos miembros del CCMT reciban capacitación sobre las funciones y las responsabilidades del equipo.

- Llevar una lista con todos los contactos clave del CCMT.

- Coordinar y divulgar el cronograma de reuniones en curso del CCMT.

2.2.3.3 Miembros del CCMT

Las responsabilidades de los miembros del CCMT (miembros principales y ad hoc) son:

- Dar prioridad a las tareas de actividades de respuesta a las crisis de acuerdo con las responsabilidades funcionales diarias durante a activación del CCMT, como lo determina el Presidente del CCMT.

- Familiarizarse por completo con sus funciones y responsabilidades individuales y con los procedimientos generales del CCMT.

- Contribuir con la pericia y los antecedentes funcionales al desarrollo de las estrategias de comunicación para las partes interesadas.

- Llevar a cabo investigaciones, reunir información y realizar otras tareas, según las asigne el Presidente del CCMT.

- Desarrollar y aprobar estrategias de gestión de crisis.

- Designar a un sustituto (que no sea parte del CCMT o del CIST) para cubrir las responsabilidades funcionales u operativas diarias cuando el CCMT esté activado.

- Participar en la capacitación y en los ejercicios.

2.2.3.4 Equipo de soporte del CCMT

Deben delegarse a dos o tres personas para que actúen como empleados de registro para reunir información clave durante las reuniones, asistir al Presidente del CCMT, responder llamadas y tomar mensajes para los miembros del CCMT. Las tareas adicionales son las siguientes:

- Tomar notas de las reuniones del CCMT y publicarlas con la orientación del asesor legal.

- Documentar las decisiones y las actividades asignadas en los formularios de seguimiento de problemas y de actividades.

- Distribuir la documentación a los miembros apropiados del equipo.

- Mantener el informe de incidentes y otras herramientas de trabajo utilizadas por el CCMT.

- Efectuar otras tareas, según lo indique el Presidente del CCMT.

2.2.4 Soporte del Gerente de Seguridad Regional

El apoyo adicional para responder a los incidentes en las instalaciones de Israriego será brindado por el Gerente de Seguridad Regional (RSM) de ISRARIEGO, quien estará a cargo de la región global en la que se encuentran las instalaciones de la empresa.

Si el IRT o el Presidente del CIST del lugar lo solicitan, el RSM puede brindar asistencia inicial en el lugar para responder al incidente. El RSM informará de inmediato al Presidente del CIST sobre el soporte del RSM que fue brindado al lugar o solicitado del lugar. El RSM proporcionará actualizaciones continuas al Presidente del CIST con respecto a las necesidades, el soporte o los pedidos del sitio.

Si no se ha activado el CIST, todas las decisiones sobre el soporte del sitio brindadas por el RSM serán tomadas por el Director de Operaciones de Seguridad Mundial tras consultar con el Presidente del CIST. Una vez activado el CIST, el RSM se transformará en un miembro ad hoc del CIST. Así, el CIST decidirá y coordinará todo el apoyo adicional del RSM que debe brindarse en el sitio.

Las comunicaciones del RSM con el sitio o el soporte a un sitio para un incidente no sustituirán el requisito obligatorio que debe cumplir el líder del IRT del sitio de notificar inicialmente al Presidente del CIST acerca de un incidente que cumpla con los criterios corporativos de notificación de incidentes.

3.0 NOTIFICACIONES E INVESTIGACIONES

Es fundamental que se informe rápidamente a la organización de gestión corporativa de crisis sobre los incidentes que posiblemente se conviertan en crisis. Los lineamientos de generación de informes y los procedimientos que se describen en esta sección se implementarán en forma global. Este proceso

pretende mejorar, y no reemplazar, los planes internos de generación de informes, los procesos y los requisitos normativos ya existentes.

3.1 NOTIFICACIONES

La mayoría de las emergencias, los incidentes y los problemas emergentes serán resueltos en el nivel de la unidad por los equipos de respuesta a incidentes, que utilizarán los planes de respuesta a emergencias, los planes ya existentes de recuperación comercial u otros planes locales para contingencias. Sin embargo, algunos incidentes, debido a su magnitud, duración, interés público, nivel de controversia o impacto financiero, pueden causar una crisis para la Empresa. Para identificar rápidamente estas posibles crisis, se utilizarán los siguientes criterios de notificación.

Este proceso de notificación de crisis no tiene como objetivo reemplazar otros requisitos de generación de informes de Israriego ya existentes con procedimientos de Cumplimiento, Medioambiente, Seguridad, Violencia en el lugar de trabajo, u otros requisitos de generación de informes entre las funciones, las regiones, las divisiones y las unidades corporativas. Estos informes deben continuar realizándose de acuerdo con las políticas y los procedimientos internos de Israriego. Sin embargo, si un incidente o una situación cumplen con los criterios de posible crisis que se enumeran a continuación, debe realizarse la siguiente notificación.

3.1.1 Notificación inicial

Los equipos de respuesta a incidentes, los gerentes de los departamentos funcionales, los Gerentes de Seguridad Regional (RSM) o cualquier otro empleado o contratista que tenga conocimiento de un incidente o una situación que pareciera cumplir con los criterios que se enumeran a continuación deben notificar de inmediato al Grupo Corporativo de Evaluaciones llamando al Centro de Seguridad Mundial de ISRARIEGO a uno de los números telefónicos que figuran a continuación:

Estos incidentes requieren notificación del Equipo de Soporte Corporativo ante Incidentes:

- Muerte relacionada con el trabajo.

- Una amenaza o problema real de salud relacionado con el trabajo que puede afectar las operaciones de la empresa por ausencia al trabajo o distracción mental de las tareas laborales.

Ejemplos:

- Sucesos que afecten la productividad debido a la distracción y el impacto emocional en los empleados, como violencia en el lugar de trabajo, muerte de un empleado destacado no relacionada con el trabajo, muerte relacionada con el trabajo o enfermedad infecciosa.

- Sucesos que afecten la productividad debido a la larga ausencia de un empleado debido a una enfermedad infecciosa o para evitar el contagio de una enfermedad infecciosa.

- Acto de terrorismo o intento de acto de terrorismo contra la Empresa.

- Secuestro o intento de secuestro de empleados de ISRARIEGO.

- Información de inteligencia de que personal de ISRARIEGO es blanco de un secuestro.

- Bombardeos, secuestros o asesinatos que se produzcan en áreas en las que opera Israriego o en áreas hacia las que viajan o en las que se encuentran los empleados.

- Acto de espionaje o intento de acto de espionaje contra ISRARIEGO.

- Posible interrupción comercial a largo plazo debido a la pérdida de instalaciones,empleados, proveedores clave o TI.

- Informe o investigación de los medios de comunicación nacionales generadaspor un incidente que afecta a ISRARIEGO.

- Guerra, revolución, conflicto armado o acciones de la policía en lugares en los que opera ISRARIEGO o a donde viajan sus empleados.

- Identificación de problemas emergentes que amenazan la imagen o la reputaciónde ISRARIEGO.

- Amenaza inminente o real de un desastre natural en el lugar donde se encuentra ISRARIEGO o en un lugar cercano.

- Manifestación de activistas en el lugar.

- Interrupción del trabajo o bloqueo del ingreso a los empleados como resultadode un problema laboral.

- Falla de las telecomunicaciones regionales.

- Problemas de productos, calidad/seguridad, cumplimiento con grandes riesgos para la imagen o la reputación de la empresa.

- Incidentes ambientales o de transporte que originan un daño para el público, el medioambiente, la continuidad comercial o la imagen o reputación de ISRARIEGO.

Esta lista no es exhaustiva. Si no está seguro de que una situación cumpla con los criterios de notificación antes mencionados, notifique al Centro de Seguridad llamando al siguiente número:

Número telefónico del Centro de Seguridad Mundial de ISRARIEGO: XXXXXX

3.1.2 Notificación al CIST

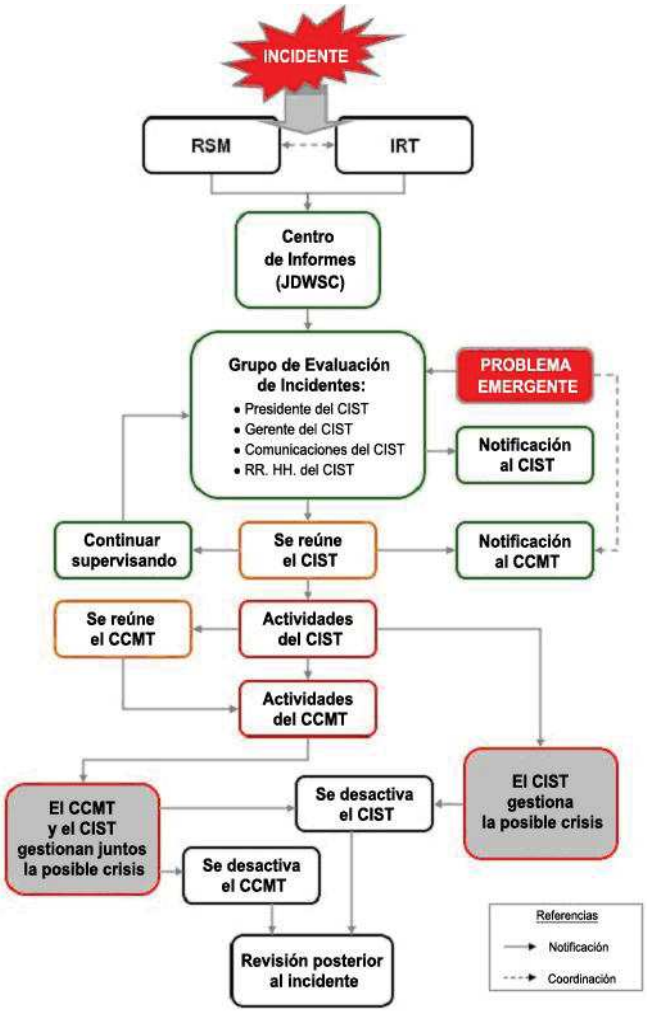
Una vez recibida la notificación inicial sobre un incidente con posible crisis, el ejecutivo de guardia notificará de forma inmediata y simultánea a los miembros del Grupo Corporativo de Evaluaciones. Este grupo está compuesto por el Presidente del CIST, el Gerente del CIST, un miembro de Comunicaciones Corporativas del CIST y un miembro de Recursos Humanos del CIST.

3.1.3 Notificación de problemas emergentes

Ciertas situaciones, por lo general, los incidentes no físicos que pueden llegar a convertirse en una crisis para ISRARIEGO, se denominan problemas emergentes.

Posiblemente, estos problemas emergentes no impliquen un único incidente diferenciado en el sitio, unidad u otro lugar físico. La notificación de un problema emergente se enviará al Grupo Corporativo de Evaluaciones (consulte, a continuación, proceso de investigación.

PROCESO DE NOTIFICACIONES E INVESTIGACIONES



3.2 INVESTIGACIÓN DE INCIDENTES

Una vez recibida la notificación inicial sobre el incidente por parte del ejecutivo de guardia, el Grupo Corporativo de Evaluaciones se reunirá e investigará el incidente para determinar si la situación justifica notificar, convocar y activar el CIST.

Si el incidente justifica que se convoque al CIST, este equipo investigará con más detalle el incidente para determinar si se debe notificar, convocar y activar el CCMT. Entre otros factores de la investigación, se utilizarán los siguientes lineamientos para determinar la continuidad de las notificaciones, reuniones y activaciones de los equipos:

LINEAMIENTOS PARA LA ACTIVACIÓN DEL CIST

- El incidente tuvo como resultado, o puede tener como resultado, un grave impacto en la imagen o marca de ISRARIEGO o puede haber generado noticias negativas.

- El incidente ha causado, o puede causar, la muerte o lesiones de empleados,ciudadanos o contratistas.

- El incidente tuvo como resultado, o puede tener como resultado, impactos fuera del lugar de trabajo o en la comunidad, como peligros para la salud o la seguridad pública o evacuación forzosa de los residentes.

- El incidente ha provocado, o puede provocar, una grave contaminación ambiental debido a la toxicidad o a la sensibilidad ecológica de la zona.

- El incidente tuvo como resultado, o puede tener como resultado, una gran interrupciónde las operaciones de ISRARIEGO, en la unidad o en otras instalaciones.

- El incidente puede tener como resultado problemas políticos, normativos o internacionales a largo plazo.

- La respuesta al incidente requerirá que la dirección se concentre en la movilización y coordinación sustancial del personal o de los recursos de ISRARIEGO, más allá de los niveles de rutina establecidos en los planes existentes para contingencias.

- El incidente puede tener graves impactos financieros o de cumplimiento legal para la empresa.

- La sensibilidad a este tipo de sucesos se ve incrementada debido a una historia de incidentes similar, ya sea en la unidad o región, dentro de la empresa o entre los miembros de nuestra industria.

Una vez que el Grupo Corporativo de Evaluaciones finaliza el proceso de investigación, el Presidente del CIST notificará al Presidente del CCMT acerca de todas las acciones que debe tomar el CIST. Esta notificación puede incluir una recomendación del Presidente del CIST al Presidente del CCMT sobre la posible notificación, convocación o activación del CCMT.

4.0 CONCEPTO DE LAS OPERACIONES

A continuación, se describe el proceso de operaciones del Equipo de Soporte Corporativo ante Incidentes (CIST) y del Equipo de Gestión Corporativa de Crisis (CCMT) de ISRARIEGO en respuesta a una posible crisis:

4.1 OPERACIONES DEL CIST Y DEL CCMT

4.1.1 Activación del CIST

Las acciones de respuesta y de restauración para las unidades locales serán llevadas a cabo por los IRT de la unidad con la ayuda del Gerente de Seguridad Regional pertinente. Los incidentes de funciones específicos serán manejados por los IRT dentro de esa función, con la ayuda del departamento funcional corporativo que corresponda. Sin embargo, cuando la gestión del incidente exija recursos que no están disponibles para los IRT funcionales o locales, pueden activarse el CIST o el CCMT para brindar el soporte corporativo de los recursos. Asimismo, si el incidente puede llegar a convertirse en una crisis para la Empresa, se activarán el CIST o el CCMT para brindar capacidades de toma de decisiones estratégicas.

Las operaciones del CIST y del CCMT comienzan con dos pasos operativos diferenciados para su participación en el proceso de gestión de crisis:

Reunión: La primera reunión física o virtual del equipo (CIST o CCMT) para llevar a cabo un análisis inicial de un incidente que se ha informado y para determinar si se necesita la activación formal del equipo u otra acción corporativa.

Activación: La primera reunión formal del equipo (CIST o CCMT) que marca el comienzo del proceso corporativo de respuesta a la crisis y de toma de decisiones; el equipo asume su autoridad en virtud de este Plan Global de Gestión de Crisis.

Una vez tomada la decisión por parte del Grupo Corporativo de Evaluaciones, el CIST se reunirá en el lugar de reunión del CIST (consulte la sección 4.3). Una vez convocado el CIST, todos los miembros de este equipo deben concurrir a la reunión inicial (consulte el ejemplo Agenda de reuniones del CIST: reunión inicial, en el Apéndice E). (Según las limitaciones de viaje o el momento del día, el Presidente del CIST puede aprobar que ciertos miembros del CIST se unan a la reunión inicial de manera remota, por teléfono u otra forma de comunicación).

Luego de la reunión inicial del CIST, el Presidente de este equipo, con la contribución de todos los miembros, llevará a cabo una de las siguientes acciones:

- Activar de inmediato el CIST para operaciones de todos los días, las 24 horas.

- Activar de inmediato el CIST para operaciones de todos los días, las 24 horas y descartar del equipo a algunos miembros del CIST si no hay problemas graves que afecten sus áreas funcionales específicas en la empresa.

- No activar el CIST, pero continuar controlando el incidente y brindando información actualizada sobre el incidente a los miembros del equipo hasta que la situación se modifique.

El Presidente del CIST también notificará al Presidente del CCMT acerca de todos los problemas importantes que surjan de la reunión del CIST, del estado del CIST y de todas las recomendaciones para la participación del CCMT.

Si se activa el CIST, los miembros de este equipo y sus suplentes deberán trabajar las 24 horas para apoyar la respuesta al incidente. Durante la reunión inicial del CIST, el Presidente determinará el cronograma de reuniones del equipo. Se programan reuniones formales del CIST para implementar un formato estructurado que permita que el CIST funcione y responda con la máxima velocidad y eficacia.

Es importante que todos los miembros del CIST o sus suplentes estén presentes en las reuniones formales mientras el CIST esté activado. La ausencia de uno solo de los miembros del CIST puede provocar graves brechas en la información y también una toma de decisiones incompleta. Para garantizar la participación total de los miembros del CIST y, no obstante, permitir interrupciones en el proceso de toma de decisiones para que los miembros asignen o

lleven a cabo acciones individuales de respuesta a incidentes, se utilizará un proceso de “encuentro-separación/ encuentro-separación” durante la activación del CIST. En la reunión inicial del CIST (la etapa de “encuentro”), el Presidente del CIST informa al equipo, analiza el incidente, identifica los problemas corporativos, toma las decisiones y asigna problemas o acciones para los miembros individuales del CIST. La duración de esta reunión será limitada (por ejemplo, no más de 2 horas). Luego de la reunión inicial, el equipo generalmente se “separará” durante aproximadamente 1 ó 2 horas, lo que permite que los miembros del CIST se reúnan con sus departamentos o grupos funcionales para implementar acciones, coordinar actividades de respuesta con el IRT y realizar investigaciones para reunir información adicional que pueda ser importante para el soporte ante el incidente. Luego, el CIST se reunirá nuevamente (“encuentro”) en el horario fijado con anterioridad para brindar informes de actualización sobre problemas asignados, actividades y la identificación de problemas o acciones nuevos o adicionales (consulte el ejemplo Agenda de reuniones del CIST: reuniones posteriores, en el Apéndice C). Este proceso de “encuentro-separación/encuentro-separación” continúa hasta que se declara la desactivación del CIST.

4.1.2 Activación del CCMT

Por lo general, la respuesta corporativa a un incidente puede estar limitada a la activación del CIST. Sin embargo, cuando la escala, la duración, los impactos reales/pronosticados o la sensibilidad del problema justifican una toma de decisiones estratégicas en el nivel más alto de la Empresa, se activará el CCMT.

Aunque la activación del CCMT no requiere que los miembros del CCMT estén disponibles las 24 horas, el Presidente del CCMT programará y llevará a cabo las reuniones, según corresponda, que exijan la presencia (o participación telefónica, si el Presidente así lo estipula) de todos los miembros de CCMT.

Puede convocarse al CCMT por recomendación del Presidente del CIST o en cualquier momento que el Presidente considere conveniente. Con los aportes de los miembros del CCMT, el Presidente del CCMT determinará la implementación de una de las siguientes acciones:

- Activar de inmediato el CCMT.

- No activar el CCMT, pero continuar recibiendo información actualizada sobre el incidente por parte del Presidente del CIST hasta que la situación se modifique.

Al igual que el formato de reuniones del CIST, las reuniones formales del CCMT se programan y se llevan a cabo en un formato estructurado para maximizar la velocidad y eficacia de respuesta del equipo. Es importante que todos los miembros del CCMT estén presentes en las reuniones formales mientras el CCMT esté activado. La ausencia de uno solo de los miembros del CCMT puede obstaculizar el proceso de toma de decisiones estratégicas del equipo y su capacidad de gestión de crisis.

Al igual que con el CIST, para garantizar la participación total de los miembros del CCMT y, no obstante, permitir interrupciones en el proceso de toma de decisiones para que los miembros asignen o lleven a cabo acciones individuales de respuesta a incidentes, también se utilizará un proceso de "encuentro-separación/encuentro-separación" durante la activación del CCMT.

En la reunión inicial del CCMT (la etapa de "encuentro"), el Presidente del CCMT informa al equipo, analiza el incidente, identifica los problemas corporativos, toma las decisiones y asigna problemas o acciones (consulte el ejemplo Agenda de reuniones del CCMT: reunión inicial, en el Apéndice E). La duración de esta reunión será limitada (por ejemplo, no más de 2 horas) para que los miembros puedan ir a comunicar las decisiones del CCMT y asignar las acciones adecuadas. Luego, el equipo generalmente se "separará" hasta que

el Presidente del CCMT determine que nuevos problemas importantes exigen que el CCMT se reúna para analizarlos y para tomar más decisiones estratégicas.

A continuación, el CCMT se reunirá nuevamente (“encuentro”) en el horario fijado con anterioridad para brindar informes de actualización y llevar a cabo la toma de decisiones (consulte el ejemplo Agenda de reuniones del CCMT: reuniones posteriores, en el Apéndice E).

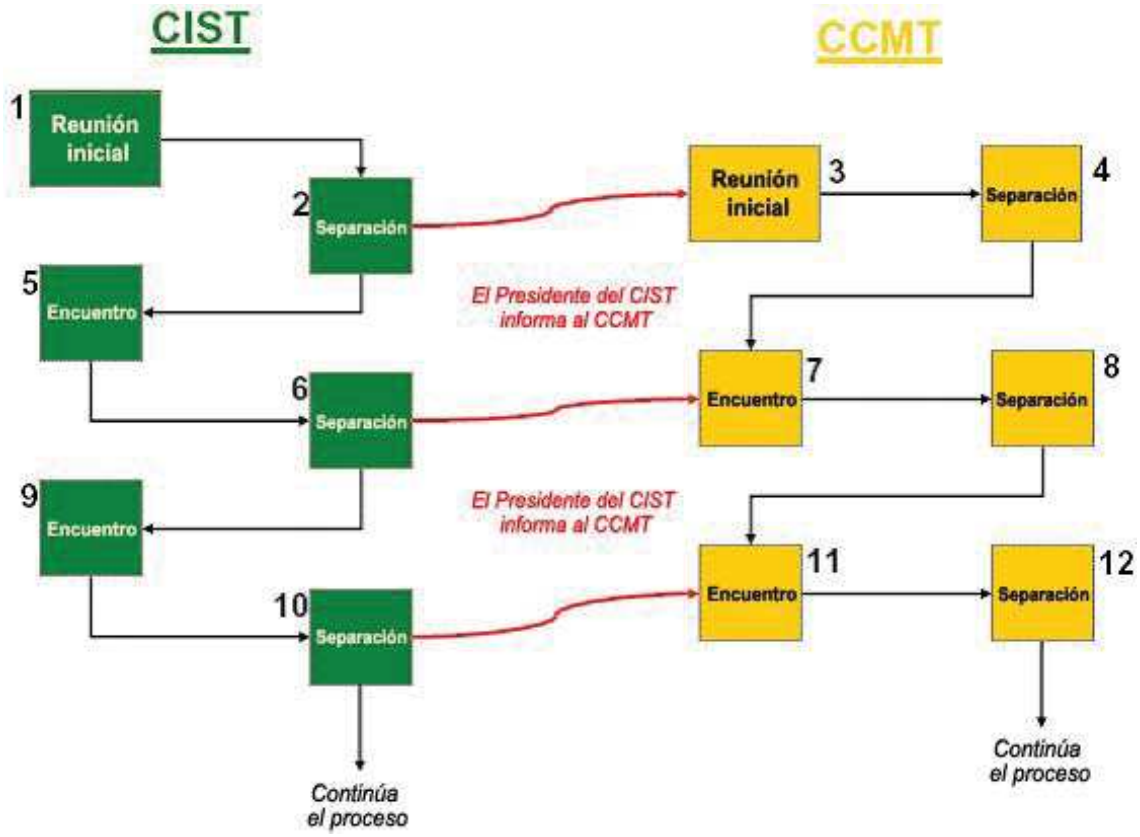
Este proceso de “encuentro-separación/encuentro-separación” continúa hasta que se declara la desactivación del CCMT.

4.2 COORDINACIÓN DE LAS REUNIONES DEL CIST Y DEL CCMT

Si se activa el CCMT, las reuniones formales del equipo se programarán para que se lleven a cabo cuando el CIST se encuentre en la etapa de “separación”.

En la figura anterior se muestra la secuencia de los procesos combinados de “encuentroseparación/encuentro-separación” del CIST y del CCMT.

Asimismo, el CCMT y el CIST deben alternar los horarios de inicio de las reuniones formales para evitar que las reuniones se lleven a cabo al mismo tiempo. Esto permitirá que el Presidente del CIST informe al CCMT y también garantizará que los equipos no tomen decisiones ni implementen acciones sin tener conocimiento de las acciones y decisiones del otro equipo. Los gerentes del CIST y del CCMT son responsables de la coordinación de los cronogramas de reuniones de los equipos.



4.3 REUNIONES Y UBICACIONES DE LOS EQUIPOS

El CIST se reunirá y funcionará desde los siguientes lugares durante la reunión o la activación del equipo:

Lugar principal de reunión del CIST: Centro de gestión de crisis
Lugar alternativo de reunión del CIST: Oficina N.º 3 - Planta baja
Segundo lugar alternativo de reunión del CIST: Sala de juntas N.º 2

Una vez reunido o activado el CCMT, el equipo se reunirá y funcionará desde las siguientes ubicaciones:

Lugar principal de reunión del CCMT: Sala de juntas del 2.º piso
Lugar alternativo de reunión del CCMT: Sala de conferencias ejecutivas
Segundo lugar alternativo de reunión del CCMT: Sala de juntas N.º 1

4.4 HERRAMIENTAS DE SEGUIMIENTO DE LA INFORMACIÓN DE CRISIS DE LOS EQUIPOS

Durante todo el proceso de gestión corporativa de crisis, se utilizarán cuatro formularios de información clave para documentar los hechos del incidente (formulario Informe de incidentes), los problemas que deben tratarse (formulario Seguimiento de problemas), las acciones que deben ponerse en práctica (formulario Estado de las actividades) y el pronóstico de las consecuencias del incidente (formulario Análisis del impacto adverso).

4.4.1 Informe de incidentes

El formulario Informe de incidentes (consulte el Apéndice F) será utilizado por el Centro de Informes para documentar los hechos iniciales relacionados con el incidente al recibir la notificación inicial. El Centro de Informes entregará de inmediato el Informe de incidentes al Grupo Corporativo de Evaluaciones.

Este formulario será la herramienta con la que contará el Centro de Informes para continuar brindando información sobre el estado del incidente al Grupo Corporativo de Evaluaciones hasta que se active el CIST. Una vez activado el CIST, el Informe de incidentes se transfiere del Centro de Informes al CIST y luego el Gerente del CIST deberá mantenerlo y actualizarlo a través de la comunicación directa con el sitio.

4.4.2 Seguimiento de problemas

Para ayudar al CIST a ocuparse sistemáticamente de los problemas en respuesta al incidente, se utilizará el formulario Seguimiento de problemas. Ésta es la herramienta principal para realizar un seguimiento de los problemas que deben enfrentar el CIST o el CCMT. El Gerente del CIST garantizará que el personal de soporte escriba y mantenga una descripción de cada problema, como identifica el CIST durante su evaluación de las consecuencias del

incidente. El CIST revisará este formulario en las reuniones siguientes para confirmar o revisar los problemas enumerados y para asignar o ajustar prioridades en el momento adecuado. Si se activa el CCMT, el Presidente del CIST utilizará el formulario Seguimiento de problemas para informar al CCMT y para hacer un seguimiento de aquellos problemas que el CCMT gestionará como “propios”. El formulario Seguimiento de problemas aparece en el Apéndice F.

4.4.3 Estado de las actividades

Para poder resolver los problemas de respuesta, suelen ser necesarias varias acciones de distintas personas o grupos funcionales. Debido a que las acciones están determinadas para abordar los problemas que surgen durante el soporte ante incidentes, se hará un seguimiento sistemático de ellas usando el formulario Estado de las actividades. Ésta es la herramienta principal para supervisar las acciones y las tareas del CIST. Cuando el CIST identifique acciones durante la determinación de las necesidades de respuesta a incidentes, el personal de soporte del CIST escribirá una descripción de cada una de las acciones que deben implementarse para responder al problema. En las reuniones siguientes, el CIST revisará este formulario para confirmar o revisar el estado de las acciones enumeradas, establecer prioridades y asignar responsabilidades de liderazgo. El Presidente del CIST también utilizará este formulario para informar al CCMT y para hacer un seguimiento del soporte del CIST al sitio. Este formulario Estado de las actividades está pensado para ser utilizado junto con el formulario Seguimiento de problemas para brindar una forma de seguimiento de la respuesta general. El formulario Estado de las actividades aparece en el Apéndice F.

4.4.4 Análisis del impacto adverso

El último formulario de información, Análisis del impacto adverso, ayuda al CIST y al CCMT a responder con anticipación a las necesidades del sitio y a

los problemas que puedan surgir más tarde durante el incidente. La información “pronosticada” que se escribe en el formulario Análisis del impacto adverso garantiza que el CIST y el CCMT tengan en cuenta las presunciones sobre el “peor resultado posible” y las consecuencias del incidente.

Inicialmente, el CIST utilizará el formulario Análisis del impacto adverso en las discusiones con el IRT para determinar la posible necesidad de acciones, activos o recursos corporativos adicionales en el futuro. Si se activa el CCMT, éste utilizará el formulario Análisis del impacto adverso y sus presunciones para realizar las primeras deliberaciones sobre posibles problemas futuros y para tomar decisiones estratégicas oportunas (Consulte el formulario Análisis del impacto adverso en el Apéndice F).

La información en el formulario Análisis del impacto adverso no se reproducirá ni divulgará, y se conservará en el formulario original. Después de presentar el formulario para el pronóstico y el análisis en una reunión del CIST o del CCMT, el único representante legal del equipo guardará y conservará la única copia del formulario.

4.5 DESACTIVACIÓN DEL CCMT Y DEL CIST

La desactivación del CCMT tendrá lugar cuando:

- No exista más la necesidad de un enfoque sustancial de dirección ejecutiva en el nivel corporativo.

- Ya no exista un beneficio de valor agregado para continuar con la activación del CCMT.

- El CCMT haya desarrollado un plan general de acción que permita que todos los problemas restantes sean gestionados eficazmente.

- Se haya determinado que el sitio afectado y el CIST pueden continuar con la gestión de las consecuencias desde ese momento sin la participación del CCMT.

- Se haya establecido una estrategia y un plan de evaluación de los desarrollos negativos y una posible reactivación de todo el CCMT o de una parte de él.

- Se haya confirmado y programado una reunión de revisión posterior al incidente.

- Se haya establecido un cronograma para actualizaciones periódicas (quincenal, mensual y trimestral) sobre el estado de la resolución continua de los impactos corporativos del incidente (si es necesario).

La desactivación del CIST tendrá lugar cuando:

- El sitio no necesite soporte ante incidentes que requiera el análisis o la coordinación colectiva del CIST.

- El sitio no necesite recursos que requieran de la coordinación colectiva del CIST.

- Se haya tratado la orientación y las decisiones para todos los problemas identificados.

- Se hayan evaluado las consecuencias del incidente y se haya desarrollado un plan para atenuar los impactos de dichas consecuencias.

- Se haya brindado un informe final y los miembros del equipo estén de acuerdo con la decisión de desactivarlo.

En virtud de la política de conservación de registros de ISRARIEGO, el departamento legal centralizará todos los registros luego de la desactivación de los equipos de respuesta.

4.6 REVISIONES POSTERIORES AL INCIDENTE

Luego de que haya concluido un incidente, se efectuará una revisión posterior al incidente. El procedimiento para la revisión será el siguiente:

- El Presidente del CIST convocará a una reunión con todos los miembros activados del equipo, con el CCMT y con el IRT pertinente antes de que transcurran 45 días desde la desactivación de los equipos.

- Se revisará toda la información relevante y los datos recopilados durante la respuesta.

- Se realizarán entrevistas con los empleados del sitio y de la empresa, los testigos o los contratistas implicados para proporcionar la información clave que no figure en las entrevistas originales.

- Se determinarán las posibles causas de la crisis.

- Se recomendarán las posibles medidas correctivas para el sitio en el que se produjo el hecho y para otros sitios que pudieran haber sido afectados por un incidente similar.

- Se revisarán el Plan de Gestión de Crisis y los procedimientos de respuesta complementarios para evaluar su eficacia y se incorporarán a este Plan.

5.0 PROGRAMA CORPORATIVO DE PREPARACIÓN DE ISRARIEGO: MANTENIMIENTO DEL PLAN, CAPACITACIÓN Y PRÁCTICA

5.1 MANTENIMIENTO DEL PLAN

Para mantener una eficaz respuesta a la crisis para ISRARIEGO, este Plan Global de Gestión de Crisis se conservará y se actualizará sistemáticamente con el fin de que refleje con claridad las capacidades, los procedimientos y los protocolos existentes de la Empresa.

Los cambios continuos en las políticas y los procedimientos de Israriego relacionados con las crisis, las mejoras en los conceptos y la tecnología de respuesta o los cambios en las normas gubernamentales se reformularán en este Plan para garantizar que siga siendo una guía de respuesta viable. Además, se examinarán las lecciones que se aprendan a partir de los ejercicios, las revisiones posteriores al incidente y los incidentes reales para evaluar si es necesario introducir modificaciones en este Plan.

Todo el Plan debe revisarse y actualizarse todos los años, como mínimo.

El Plan también debe estar sujeto a revisión y actualización después de que un incidente o una crisis real produzcan la activación del CIST o del CCMT, y también después de actividades de ejercitación y simulacros importantes.

Los cambios que se consideren fundamentales para la adecuación del Plan deben incorporarse inmediatamente, en lugar de esperar a incluirlos en la actualización anual programada.

Los materiales de recursos desarrollados para respaldar el plan (por ejemplo, las listas de funciones y los apéndices) deben revisarse y actualizarse trimestralmente, debido a la naturaleza de la información que contienen.

5.2 REUNIONES ORDINARIAS DE LOS EQUIPOS

Tanto el CIST como el CCMT llevarán a cabo reuniones ordinarias para garantizar que el equipo esté familiarizado con sus funciones y para mantener la cohesión entre sus miembros.

5.2.1 REUNIONES DEL CCMT

El CCMT se reunirá regularmente dos veces al año, aproximadamente cada seis meses. El Presidente del CCMT dirigirá la reunión e incluirá en la agenda una revisión de las actividades del programa de gestión de crisis y también revisiones estructuradas posteriores al incidente de situaciones reales que hayan ocurrido después de la última reunión. Cuando corresponda, la reunión del CCMT también incluirá una descripción, basada en situaciones, del Plan Global de Gestión de Crisis, que se centrará en la función del CCMT y en sus responsabilidades. Una activación real del CCMT para una posible crisis o la activación simulada del CCMT para un ejercicio de crisis también serán parte de esta reunión semestral del CCMT.

5.2.2 REUNIONES DEL CIST

El CIST se reunirá trimestralmente en forma regular. El Presidente del CIST dirigirá la reunión e incluirá en la agenda una revisión de las actividades del programa de gestión de crisis y también revisiones estructuradas posteriores al incidente de situaciones reales que hayan ocurrido después de la última reunión. Cuando corresponda, la reunión del CIST también incluirá una descripción, basada en situaciones, del Plan Global de Gestión de Crisis, que se centrará en la función del CIST y en sus responsabilidades. Una activación real del CIST para una posible crisis o la activación simulada del CIST para un ejercicio de crisis también serán parte de esta reunión trimestral del CIST.

5.3 CAPACITACIÓN

Para que este Plan documente con exactitud y oriente eficazmente a ISRARIEGO para la respuesta a una posible crisis, debe estar acompañado por un programa de capacitación continua para los miembros del CCMT y del CIST.

5.3.1 CAPACITACIÓN DEL CCMT

Los miembros del CCMT participarán en un curso de capacitación inicial y de un curso anual de actualización sobre el Plan Global de Gestión de Crisis y sobre sus funciones y responsabilidades en virtud de dicho Plan.

5.3.2 CAPACITACIÓN DEL CIST

Los miembros del CIST y los suplentes participarán de un curso de capacitación inicial y de un curso anual de actualización sobre el Plan Global de Gestión de Crisis y sobre sus funciones y responsabilidades en virtud de dicho Plan.

5.4 PRÁCTICA

Este Plan se validará a través de un programa continuo de ejercicios de gestión de crisis. Los ejercicios de gestión de crisis se llevarán a cabo con la participación de un solo equipo de respuesta (es decir, el CIST), con más de un equipo de respuesta (es decir, el CIST y el CCMT) o con todos los equipos de respuesta (el CIST, el CCMT y el IRT).

Se llevarán a cabo tres tipos de ejercicios básicos:

Ejercicios prácticos: Ejercicios basados en situaciones para que uno o más equipos de gestión de crisis o de respuesta ante emergencias que utilizan una

discusión dirigida para analizar una o más situaciones hipotéticas, definan la política de gestión de crisis y validen el Plan Global de Gestión de Crisis de ISRARIEGO.

Simulacros: Un ejercicio basado en situaciones, de una duración de cuatro a seis horas, en el que los miembros del equipo de respuesta demuestran sus capacidades grupales e individuales para la gestión de crisis. En este tipo de ejercicio, se utiliza una “celda de simulación” para recrear toda la interacción externa con entidades que no participan en el simulacro.

Ejercicios integrales: Un ejercicio basado en situaciones, de una duración de seis a doce horas, en el que participan todos los niveles de la estructura de gestión de crisis y de respuesta ante emergencias de ISRARIEGO, con el fin de proporcionar una validación integral de las capacidades de gestión de crisis de la empresa. Los miembros del equipo de respuesta demuestran sus capacidades grupales e individuales de gestión de crisis en tiempo real, a la vez que validan los vínculos entre los distintos equipos de respuesta de ISRARIEGO y las entidades de respuesta externa.

Tanto el CIST como el CCMT participarán al menos en uno de los tipos de ejercicios arriba mencionados cada seis a nueve meses.

Específicamente, el CIST participará en un ejercicio práctico de gestión de crisis al menos una vez al año. El CIST participará en un simulacro o en un ejercicio integral al menos una vez cada 12 a 18 meses.

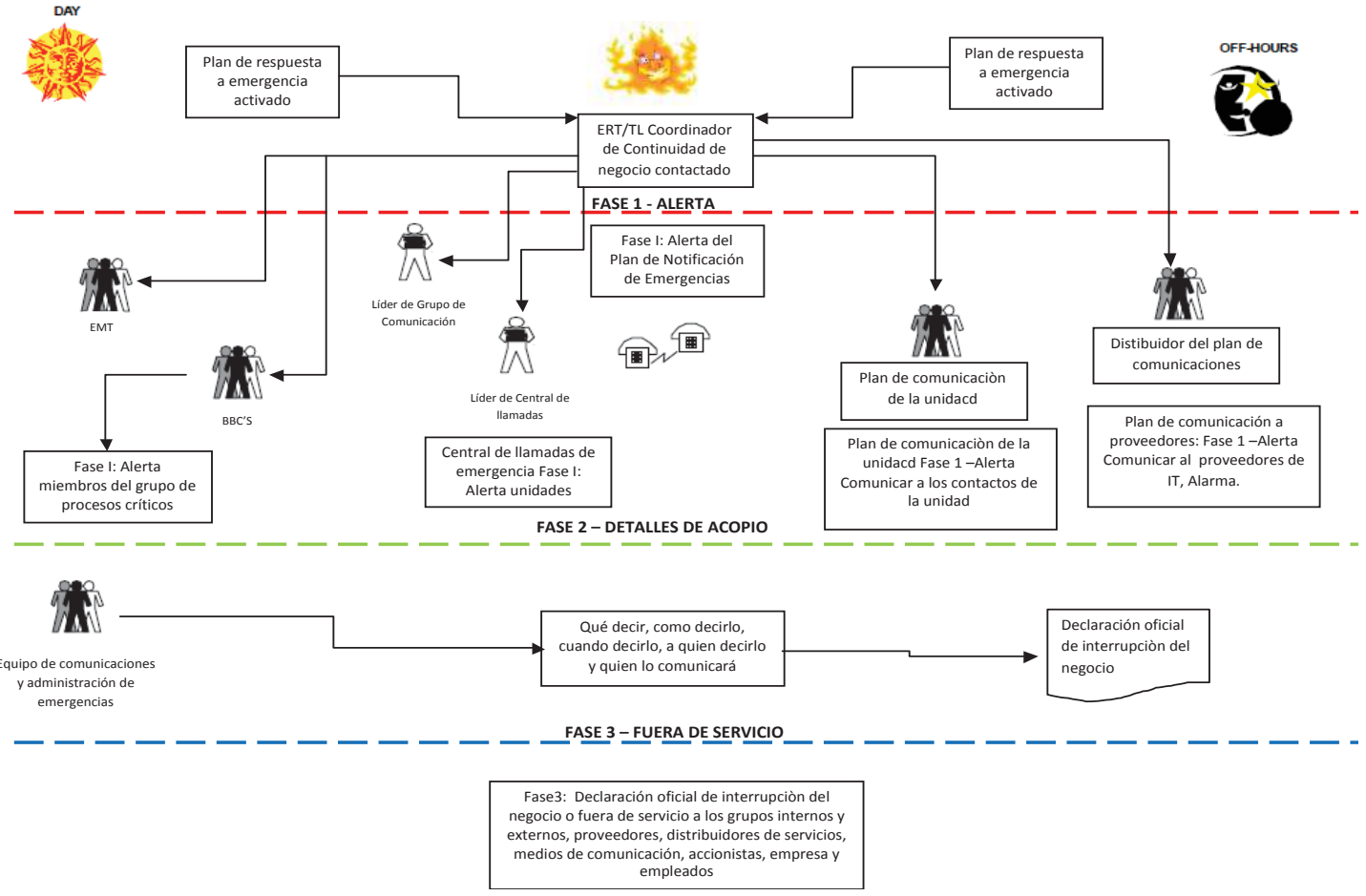
El CCMT participará en un ejercicio práctico de gestión de crisis al menos una vez al año. El CCMT participará en un simulacro o ejercicio integral al menos una vez cada 12 a 18 meses.

Al menos cada año por medio, el CCMT participará en un simulacro o ejercicio integral con el CIST y el IRT.

ANEXO 6

MAPA DE COMUNICACIONES PARA INTERRUPCIÓN DE NEGOCIOS

COMUNICACIÓN PARA INTERRUPCIÓN DE NEGOCIOS



ANEXO 7

LISTA DE VERIFICACIÓN DE COMUNICACIÓN DE CRISIS

Comunicaciones de Crisis – Preparación de lista de verificación.

Estos diez elementos deben estar en su lugar antes de una situación de crisis. Esto es de gran ayuda para mantener la compostura y ser capaz de concentrarse en su principal prioridad, el plan de respuesta a la crisis.

1. **Política y procedimientos de relaciones públicas.-** Una declaración del mandato, los valores y el programa de liderazgo.

2. **Plan de acción para comunicación de crisis.-** la gente clave, los roles, las secuencias de acción, los escenarios.

3. **Radiografía de la empresa, Información sobre Israriego y su estado.-** Este podría ser un informe anual.

4. **"Ventana": la información en la unidad -** Contenido y estar al día es lo más importante, impresos en papel con membrete Israriego. Estos documentos pueden ser entregados a los medios de comunicación para asegurar que no falta información.

5. **Archivos de referencia sobre los escenarios potenciales de crisis.-** Actas, informes, recortes – ordenado y transportable.

6. **Lista de personas clave (Key person).-** detalle ordenado y transportable, número telefónico de Trabajo y de la casa. Una página de resumen con datos de direcciones de trabajo y domicilio del personal

7. **Vocero designado (s)**

   - Establecer las personas y asignaciones previo a la crisis - principal y dos suplentes.

   - Todos deben tener algo de experiencia para hablar en público.

   - El Portavoz (s) y su asesor de relaciones públicas deben conocerse.

8. **Designados en los medios de coordinación.-** Esta función debe ser establecido como creíble y útil, tanto con su personal y los medios de comunicación antes de la crisis. La confianza es un activo excepcional en medio del caos.

9. **Directorio de medios o lista detallada.-** Usted debe tener una lista concisa de los principales medios de comunicación y su asesor de relaciones públicas en el país con sus portavoces clave.

10. **Registro de contacto para los medios.-** Usted puede tener una docena o más de los periódicos y emisoras de radio y televisión al mismo tiempo.

    - Mantenga una hoja de seguimiento individual para cada periodista / historia.

    - Sepa con quién se contactó, cuándo, qué, cómo comunicarse con ellos, cuál es su fecha límite, lo que prometió, lo que ha delegado, cuando están por llegar de nuevo a usted, si usted necesita hacer un seguimiento.

ANEXO 8

COMUNICACIÓN A EMPLEADOS DE ALERTA DE CRISIS

Formato de notificación

Fecha:
Dirección
Asunto: Incidente crítico/ Continuación del negocio
Estimado señor o señora:,
Debido a acontencimientos que van mas allá de nuestro control, Israriego es actualmente sujeto a una pérdida *[parcial / total]* de *[Información, Red (IPN) / Entorno local de red (LAN) / instalaciones, personal]*. Esperamos que este incidente afecte a nuestro negocio por los siguientes *[nùmero de]* días.
Esto no es una situación habitual del negocio, pero hemos hecho preparativos para proporcionarle el apoyo a usted y sus clientes, y funcionaremos según nuestro Plan de Continuación de negocio. Nuestro objetivo es de restaurar nuestras instalaciones cuanto antes, entonces podemos reasumir operaciones "normales" de negocio.
Mientras tanto, nuestras oficinas se esforzarán para ayudarle a usted durante esta interrupción. Israriego le mantendrá informado sobre el estado de recuperación. Si usted tiene cualquier pregunta, póngase en contacto con nosotros. Por favor refiérase a la siguiente lista para encontrar el contacto apropiado para su petición:

Contacto	Teléfono	E-Mail
Gerencia		
XXXXXXX	XXXXXXXX	XXXXXXXXX
Finanzas y Contabilidad		
XXXXXXX	XXXXXXXX	XXXXXXXXX
Recursos Humanos		
XXXXXXX	XXXXXXXX	XXXXXXXXX
Producción		
XXXXXXX	XXXXXXXX	XXXXXXXXX
Ventas		
XXXXXXX	XXXXXXXX	XXXXXXXXX
Marketing		
XXXXXXX	XXXXXXXX	XXXXXXXXX

Pedimos su comprensión debido a que bajo estas circunstancias las respuestas pueden demorar.

Atentamente.
XXXXXXXX
XXXXXXXX (Cargo)

Listado de contactos externos e internos a ser contactados

- En caso de desastre en la unidad de, los contactos de (Cliente Clave, Proveedor y Otras Listas de Contactos) de la necesidad de Plan de Continuidad de negocio - podrían tener que ser notificados sobre la interrupción.

- Si realmente un contacto tiene que ser notificado inmediatamente depende de criticidad de cada contacto. Los contactos han sido agrupados según criticidad, por favor verificar la columna " grupo" del documento de contacto

- Para notificar los contactos, use la plantilla anterior.

- Los departamentos responsables de la notificación de cada contacto son llamados en primer lugar.

ANEXO 9

CONTACTOS OFICIALES DE PRIMEROS AUXILIOS

CONTACTOS DE PRIMEROS AUXILIOS

Nombre	Ubicación	Extensión-Celular

DETALLE DE CONTACTOS DE EMERGENCIA

AMBULANCIA: 131

POLICÍA: 101

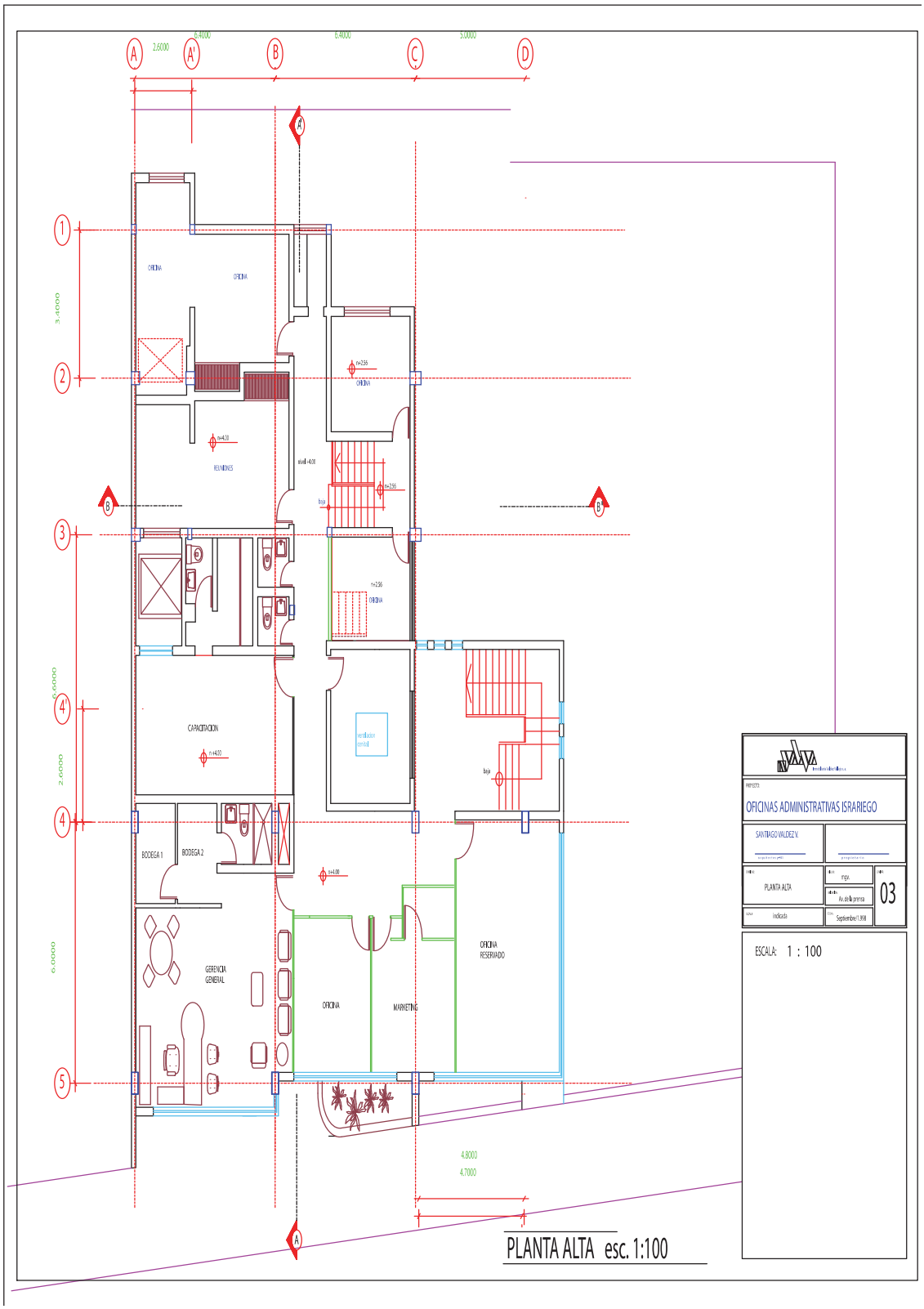
BOMBEROS: 102

CENTRO DE CONTROL DE ENVENENAMIENTO

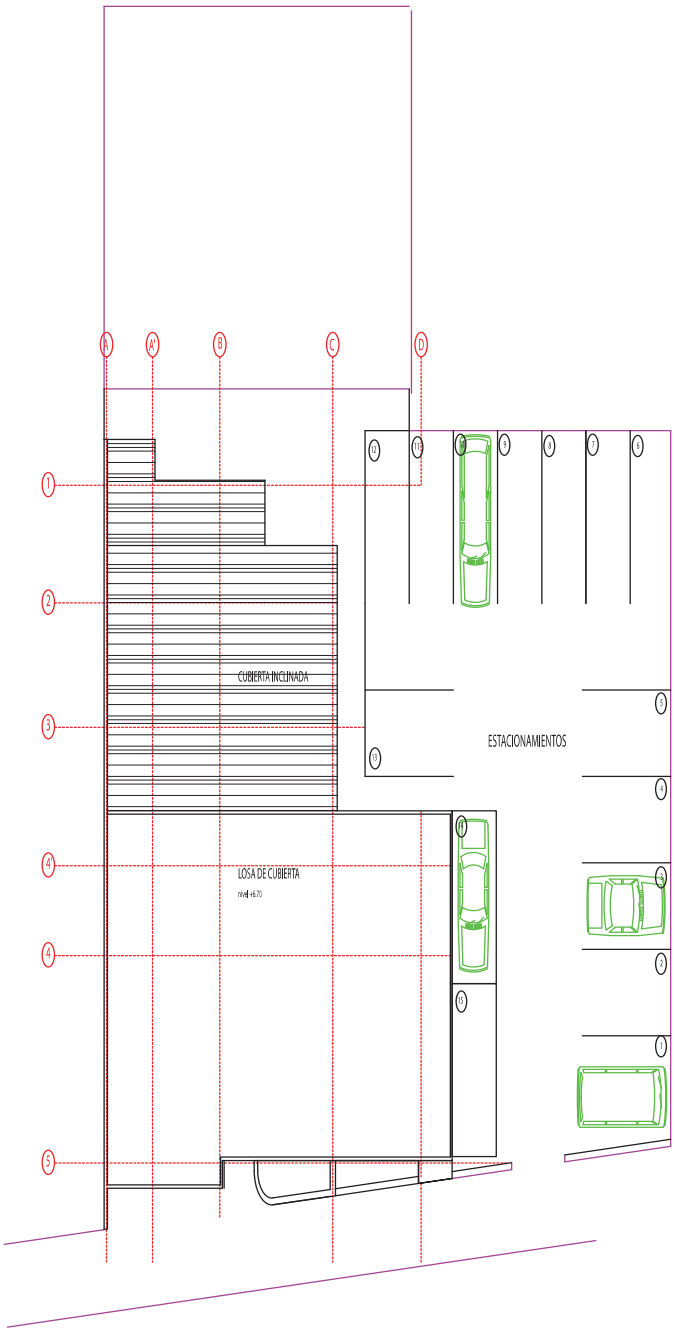
LLAMAR (911- General, defensa civil)

ANEXO 10

PLANOS OFICINAS



Planos Oficinas Quito



IMPLANTACION esc. 1:100

PROYECTO:
OFICINAS ADMINISTRATIVAS ISRARIEGO

SANTIAGO VALDEZ V.

IMPLANTACION

mgs.

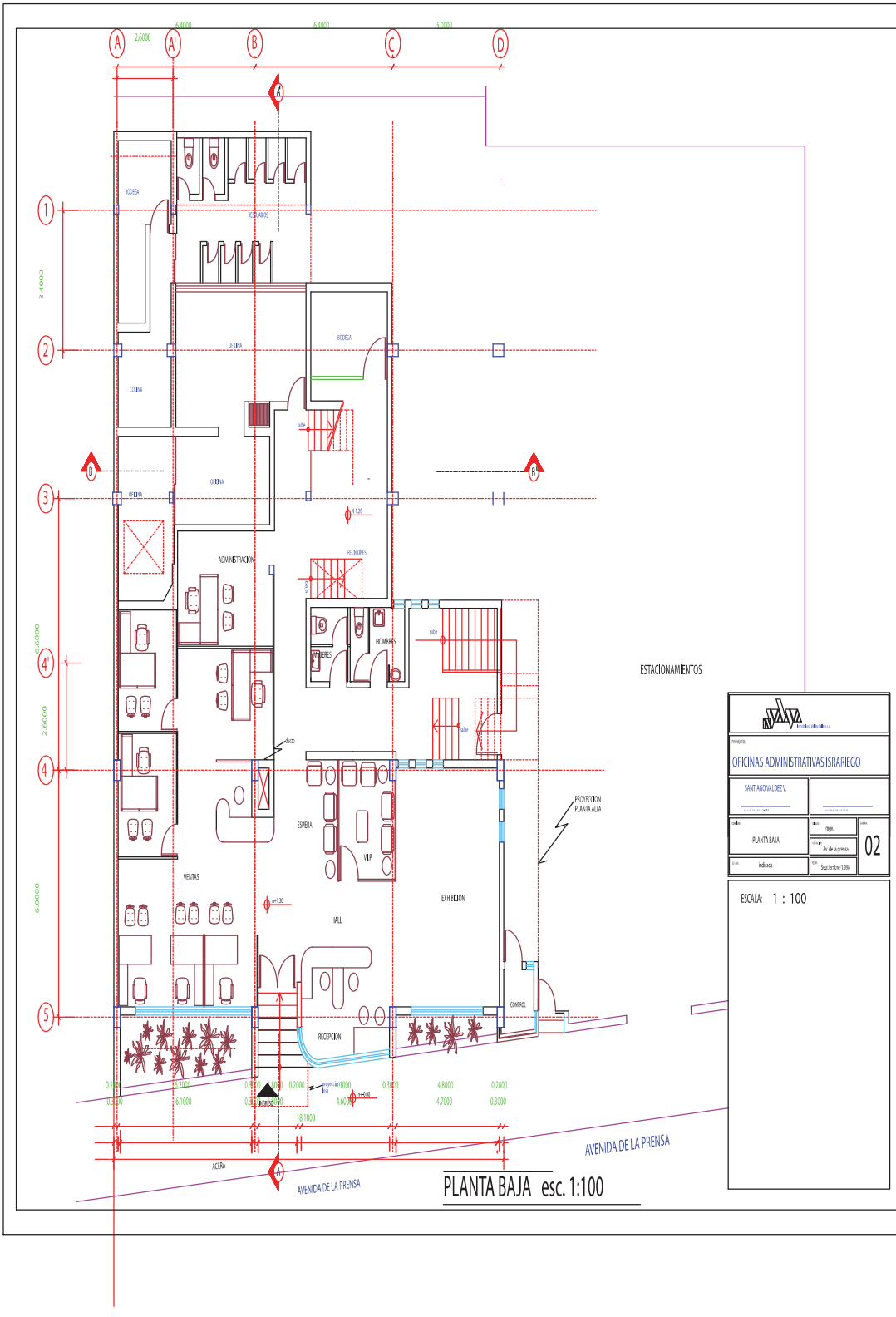
Av. de la prensa

Septiembre/1.998

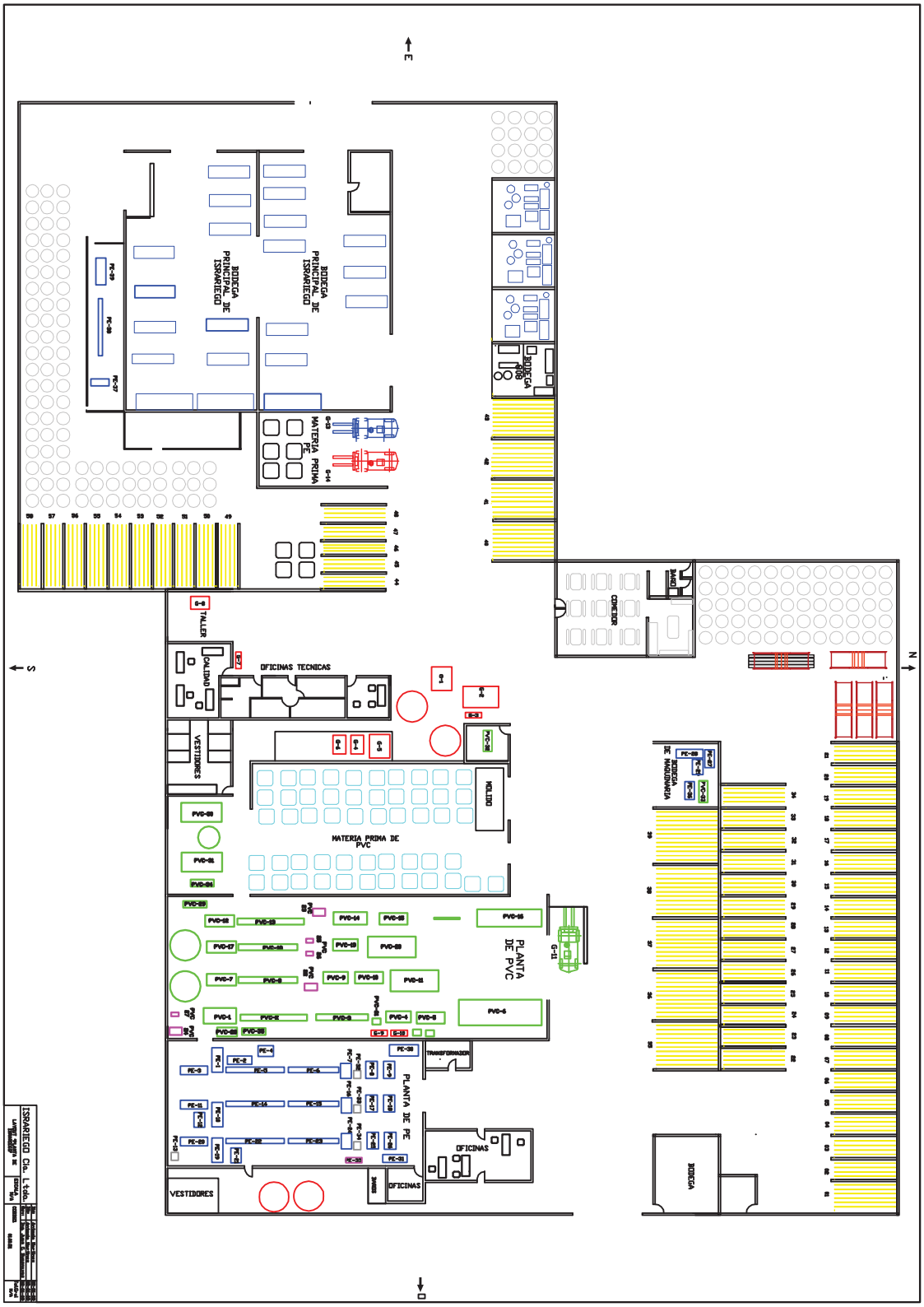
01

indicado

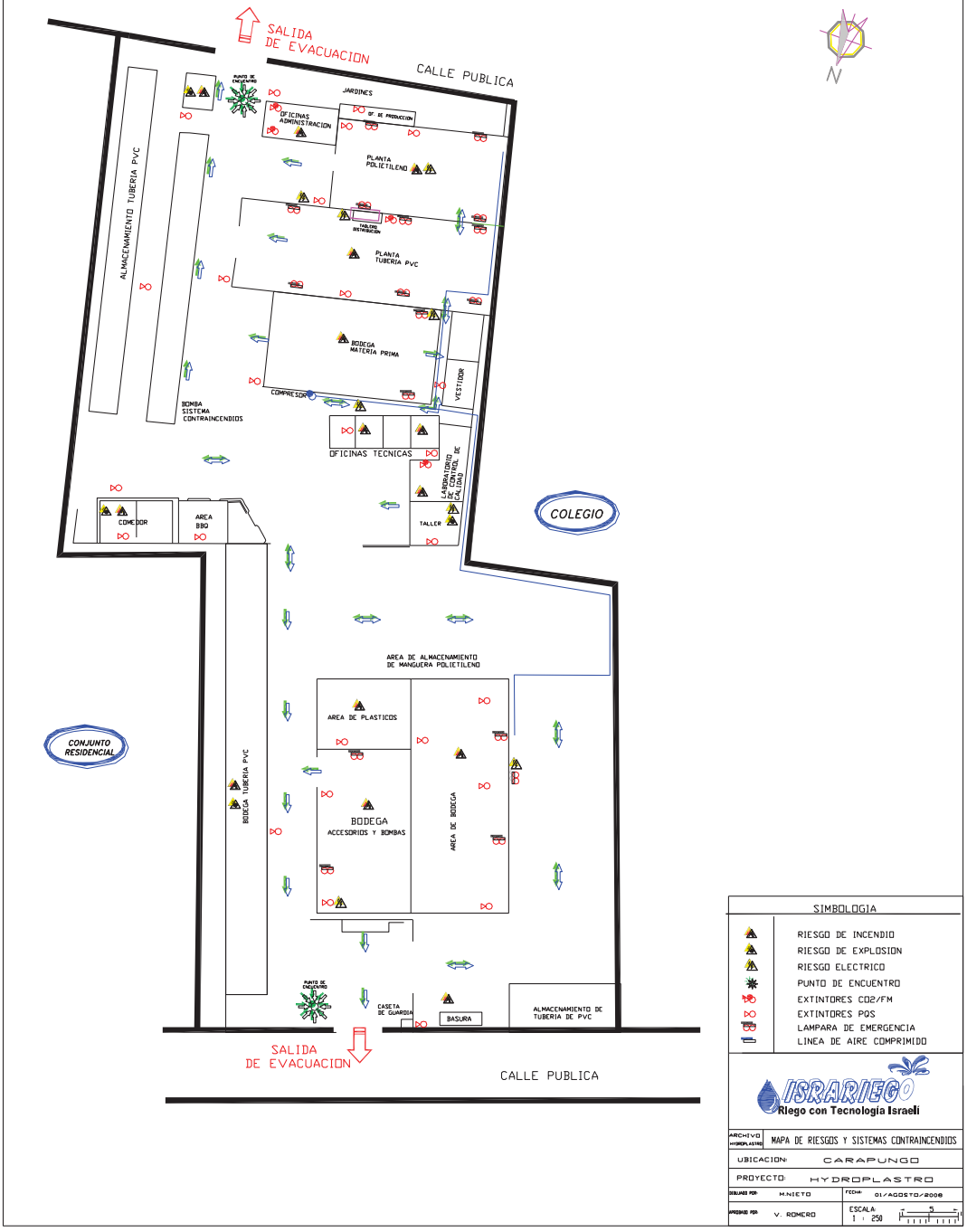
ESCALA: 1 : 100


A
A'
B
C
D
1
2
3
4'
4
5
6.4000
6.4000
5.0000
2.6000
3.4000
6.0000
2.6000
6.0000
BODEGA
RESTAURANTE
COCINA
OFICINA
ADMINISTRACION
RELACIONES
HOMBRES
MUJERES
ESPERA
V.I.P.
VENTAS
HALL
EXHIBICION
RECEPCION
CONTROL
ESTACIONAMIENTOS
PROYECCION PLANTA ALTA
ACERA
AVENIDA DE LA PRENSA
AVENIDA DE LA PRENSA
PLANTA BAJA esc. 1:100
PROYECTO:
OFICINAS ADMINISTRATIVAS ISRARIEGO
SANTIAGO VALDEZ V.
PLANTA BAJA
mapa
Av. de la prensa
Indicada
Septiembre 1/2012
02
ESCALA: 1 : 100

Plano Fábrica



Plan de Evacuación



ANEXO 11

PLAN DE RECUPERACIÓN DE DESASTRES (CDRP)

Aprobación del Plan

Las siguientes firmas de aprobación se han obtenido antes de la emisión este plan:

Grace Salazar IT Supervisor – CDRP Coordinator	Firma	Fecha
Controller	Firma	Fecha

Ubicación del Plan

Como medida de protección y rápida disponibilidad, existirán 4 copias (impresas en papel) y/o digitales (en CD) de este Plan DRP.

Cada una de las copias del Plan deben ser actualizadas en forma simultánea, y debe estar registrada su ubicación en esta página del documento.

Las copias disponibles del Plan DRP están disponibles en las siguientes ubicaciones:

COPIA 1 (copia Digital)
Ubicado en la Red LAN, en la siguiente ubicación:
//servidor1/sistemas/department/CDRP

COPIA 2 (copia Impresa y en CD)
Departamento IT Quito – Responsable: DRP Coordinator
COPIA 3 (copia Digital)

Caja Fuerte Tesorería – Oficinas Quito
Av. Prensa N50-41 y Manuel Valdivieso
Teléfono: 00593 - (2) 2468770

COPIA 4 (copia impresa y en CD)
Oficinas Guayaquil
Km 4.5 Via Daule y Amadeo Moreira - Guayaquil
Teléfono: 00593 - (4) 2350544

Introducción

Este documento es el Plan de Recuperación de Desastres (DRP) para el Data Center de Israriego Cia Ltda., ubicado en Av. La Prensa N50-41, y Manuel Valdivieso, Quito - Ecuador. La presente información en este plan guía a la dirección de la empresa y al personal técnico del área de Sistemas en la recuperación de las funciones de procesamiento de los datos y servicios del área de Informática, en el caso de un desastre que destruya todos o parte de los recursos.

Descripción

El Plan de Recuperación de Desastres está compuesto de un número de secciones que documentan los recursos y procedimientos a ser usados en la eventualidad que un desastre ocurra en las instalaciones del Data Center del

área de Sistemas. Cada plataforma de procesamiento soportada tiene una sección específica, los procedimientos de recuperación. Existen también secciones que documentan el personal que será necesario para realizar las tareas de recuperación y una estructura organizacional para el proceso de recuperación.

Información general del Plan

A través de los años, la dependencia del uso de computadoras en las actividades comerciales diarias de muchas organizaciones se ha vuelto la norma. Israriego Cia. Ltda. no es ciertamente ninguna excepción a esta tendencia. Hoy pueden encontrarse las computadoras en cada departamento de la organización. Estas máquinas están unidas por una red que proporciona comunicación con otras máquinas de la organización y con el resto de los equipos de la organización dentro y fuera del país. Las funciones vitales de la organización dependen de la disponibilidad de esta red de computadoras.

Debe considerarse por un momento el impacto de un desastre que impida el uso del sistema de Producción, Liquidación de sueldos, Contabilidad, Pago de proveedores o cualquier otra aplicación vital, durante días o semanas. Es difícil estimar el daño a la organización que un evento de estas características podría causar. Un incidente producido, por ejemplo por un incendio en las instalaciones del Data Center, podría causar un daño considerable limitando o inutilizando éstas u otras funciones vitales de la Organización. Los sistemas de procesamiento centrales de la organización podrían no estar disponibles por muchas semanas.

Objetivos y visión general

Enfoque Primario del Plan

El enfoque primario de este documento es proporcionar un plan para responder a un desastre que destruye o dañe severamente los sistemas de procesamiento centrales de la Organización operados por el área de Sistemas. El objetivo es restaurar las funciones de procesamiento tan rápidamente como sea posible, con los últimos y más actualizados datos disponibles.

Todos los planes de recuperación de desastre asumen una cierta cantidad de riesgos, el primario es cuántos de los datos están perdidos en caso de un desastre. El planeamiento de la recuperación de desastres es como el negocio del seguro, en cierta forma. Hay compromisos entre la cantidad de tiempo, esfuerzos y dinero gastado en la planificación y preparación para la recuperación ante un desastre y la cantidad de pérdida de los datos para que pueda sostener las operaciones de la organización después de un desastre. El tiempo también entra en la ecuación. Muchas organizaciones simplemente no pueden funcionar sin las computadoras que son necesarias para continuar en el negocio. Así que sus esfuerzos de recuperación pueden enfocarse en la recuperación rápida, o incluso minimizar el tiempo, reproduciendo y manteniendo sus sistemas de computadoras en medios separados.

Objetivos Primarios del Plan

Este plan de recuperación de desastre tiene los siguientes objetivos primarios:

- Presentar un curso de acción ordenado para la recuperación de la capacidad de procesamiento del Data Center del área de Sistemas.

- Proveer información sobre el personal que será necesario para llevar adelante el Plan y su especialización requerida.

- Detallar el equipamiento, software, procedimientos, diagramas de planta descriptivos, y otros ítems necesarios para llevar adelante la recuperación.

Visión general del Plan

Personal

Inmediatamente después del desastre, comienza una sucesión planeada de eventos. El personal clave es notificado y son agrupados los equipos de recuperación para llevar a cabo el plan. El personal actualmente utilizado es detallado en el plan. Sin embargo, el plan se ha diseñado para ser utilizado aun cuando algunos o todo el personal no está disponible.

En un desastre debe recordarse que las PERSONAS son el recurso más valioso. El personal de recuperación que trabaja para restaurar los sistemas de información probablemente estará realizando la tarea con un gran sacrificio personal, sobre todo en las primeras horas y los días que siguen el desastre. Ellos pueden tener lesiones que entorpecen sus habilidades físicas. La pérdida o lesión de un ser amado o compañero de trabajo pueden afectar su habilidad emocional. Además, ellos tendrán necesidades físicas por comida, abrigo y descanso.

La organización debe tomar especial atención sobre las necesidades físicas y emocionales del personal, para asegurar que quienes trabajan en la recuperación tengan los recursos necesarios disponibles. Este plan requiere la designación de una persona en el Equipo de Apoyo Administrativo cuyo trabajo será afianzar estos recursos para que ellos puedan concentrarse en su tarea.

Operaciones de Rescate en el Sitio del Desastre

Los esfuerzos iniciales están centrados en la protección y conservación del equipamiento de informática (Hardware) existente. En particular, cualquier medio magnético de almacenamiento (unidades de disco duro, cintas magnéticas, disquetes, etc.) es identificado y protegido o alejado en un ambiente limpio y seco, fuera del sitio del desastre.

Designación del sitio de recuperación

Al mismo tiempo, un estudio de la escena del desastre es realizado por el personal apropiado para estimar la cantidad de tiempo exigida para poner las instalaciones (en este caso, el edificio, recursos de hardware y software, cableado, etc.) nuevamente disponibles. Una decisión a tomar es la utilización de un sitio alternativo, a una distancia prudente de la escena del desastre, dónde puedan conectarse puestos de red y realizar el proceso en forma temporal hasta que pueda rehabilitarse el sitio primario. El trabajo de reparar o reconstruir el sitio primario empieza casi inmediatamente. Esto puede tomar semanas o meses, y los detalles están más allá del alcance de este documento.

Compra del nuevo equipamiento

El proceso de recuperación confía fuertemente en terceras partes (proveedores de software, hardware, soporte técnico, etc.), para proveer rápidamente los reemplazos de los recursos que no pueden salvarse de los daños. La Organización contará con métodos alternativos de adquisición de emergencia, para permitir que la oficina de Compras pueda hacer rápidamente los pedidos de equipos, suministros, software, y cualquier otra necesidad.

Inicio de la reinstalación en el sitio de recuperación

Los componentes nuevos y recuperados son reensamblados en el sitio de recuperación según las instrucciones contenidas en este plan. Todos los planes de este tipo están sujetos a los cambios inherentes que ocurren en la industria de la informática, por lo que puede ser necesario que el personal de recuperación tenga que desviarse del plan original, sobre todo si el plan no ha sido actualizado. Si los proveedores no pueden proporcionar una parte de un equipo en forma oportuna, puede ser necesario que el personal de recuperación tenga que hacer substituciones de último momento. Después que la fase de reensamble de equipos está completa, el trabajo se vuelve a concentrar en los procedimientos de recuperación de los datos.

Recuperación de datos desde los backups

La recuperación de los datos cuenta completamente con el uso de los backups almacenados fuera del sitio del área de Sistemas. Los backups pueden tomar la forma de cintas magnéticas, CDROM, unidades de disco, y otros medios magnéticos de almacenamiento. Los esfuerzos de recuperación de datos iniciales están enfocados en restaurar el sistema operativo para cada Servidor. Luego, en primer lugar, la recuperación de la aplicación y los datos del usuario desde los backups. Los dueños de la aplicación deben estar involucrados a esta altura del plan, para lo cual equipos de personas son asignadas por cada aplicación crítica, para asegurar que los datos se restauran apropiadamente.

Recuperación de datos de los aplicativos

Es en este punto en que el Plan de Recuperación de Desastres planificado para los usuarios y departamentos (por ejemplo, los dueños de la aplicación) debe fusionarse con el Plan de Servicios de Informática. Puesto que a pasado un determinado tiempo entre el momento de la generación de los backups y el suceso del desastre en el Data Center, los dueños de la aplicación deben tener

los recursos (ej. respaldo en papel) para restaurar los datos de la aplicación desde el momento del desastre. Ellos también deben tomar todos los datos recogidos desde ese punto y deben ingresarlo en las bases de datos de la aplicación. Cuando este proceso está completo, los sistemas de la Organización pueden volver a estar disponibles. Algunas aplicaciones sólo pueden estar disponibles a una limitada cantidad de personas clave, mientras que otros pueden estar disponibles para cualquiera que pueda acceder.

Descripción de los recursos IT actuales

Evaluación de Aplicaciones y Servicios

La siguiente tabla detalla los procesos, el tiempo de recuperación (RTO) esperado por cada responsable de los procesos y la identificación de los responsables.

Quito

Proceso	RTO (días)	Responsable	Responsable Alternativo
Finanzas & Contabilidad	4	Controller	Contador
Ventas	3	Jefe de Ventas	Vendedor
Comercio Exterior	8	Jefe Logistica	Auxiliar Compras
Diseño	3	Jefe Diseño	Auxiliar Diseño

Carapungo

Proceso	RTO (días)	Responsable	Responsable Alternativo
Bodega	8	Jefe Bodega	Auxiliar Compras 1
Compras	8	Jefe Compras	Auxiliar Compras 2
Gerencia de RRHH	15	Jefe RRHH	Auxliar RRHH
Servicio Técnico	8	Jefe Instalación	Instalador 1
Ventas a Distribuidores	3	Jefe Distribuidores	Vendedor 2

Guayaquil

Proceso	RTO (días)	Responsable	Responsable Alternativo
Diseño	3	Jefe Diseño GYE	Jefe Diseño QUlto
Comercial	3	Jefe Ventas	Jefe Diseño
Finanzas	3	Controller	Contador

Clasificación de las aplicaciones

Quito

Aplicación	Área	Usuario Responsable	Prioridad
Movex	Aplicativo para administrar las tareas de la unidad	Grace Salazar	1
LM Tool	Aplicativo para licencias de Autocad	Diego Mendoza	1
WCADI	Aplicativo para desarrollo de planos diseño	Diego Mendoza	1

Carapungo

Aplicación	Área	Usuario Responsable	Prioridad
Movex	Aplicativo para administrar las tareas de la unidad	Grace Salazar	1
Portal Distribuidores	Aplicativo Web para subir al sistema pedidos, obtener estados de cuenta, picking lists, etc.	Diego Mendoza	1

Guayaquil

Aplicación	Área	Usuario Responsable	Prioridad
Movex	Aplicativo para administrar las tareas de la unidad	Grace Salazar	1
LM Tool	Aplicativo para licencias de Autocad	Diego Mendoza	1

Clasificación de los servicios

Servicio	Descripción	Usuario Responsable	Plataforma	Prioridad
Enlaces LAN/WAN	Conexión con los equipos locales y externos a traves de la Red.	Global Infrastructure Service	N/A	1
Central Telefónica	Comunicación interna y externa	Christian Román	N/A	1
Impresión	Impresión de la documentación	Global Infrastructure Service	Windows	2

Clasificación de los servicios en Otras Unidades

Servicio	Descripción	Usuario Responsable	Plataforma	Prioridad
Active Directory	Servicio de autenticación y acceso a la red	Global Infrastructure Service	Windows	1
Monitoreo del Datacenter	Monitoreo de los servidores y enlaces	Global Infrastructure Service	Windows	3
Correo Electrónico	Servicio de correo electrónico sobre exchange	Global Infrastructure Service	N/A	2
MOVEX	Aplicativo para administrar las tareas de la unidad	Grace Salazar	OS400	1

Detalle de los recursos de Hardware

En la siguiente planilla Excel están inventariados los recursos de hardware instalados en el Data Center de la Unidad.

Detalle de Equipos por Unidad

Servidores

Se detallan los ejemplos de cada equipo a detallarse:

Nombre	Rol	Marca	Modelo	Sistema Operativo	Procesador	Espacio en Disco	Memoria RAM	Fuentes	Prioridad
Ejemplo Servidor	Archivos, impresión y servicios de red	HP	HP Proliant DL 380G5	Windows 2003	Intel Xeon E5420	C:\ ==> 136 GB D:\ ==> 683 GB	3,25 GB	2	1

Equipamiento LAN

Nombre	Marca	Modelo	Sist. Operat.	Procesador	Espacio en Disco	Memoria RAM	Fuentes	Prioridad
Ejemplo	HP	HP 1/8 G2 Tape	Windows 2003	N/a	N/a	N/a	1	1

Equipamiento WAN

Nombre	Marca	Modelo	Sistema Operativo	Procesador	Espacio en Disco	Memoria RAM	Fuentes	Prioridad
Ejemplo Router	Cisco	Cisco 2811	IOS	N/a	N/a	N/a	1	1

Contactos de Proveedores

Proveedor	Marca/Producto	Nombre	Dirección	Tlf Oficina	Critico?
Ejemplo Proveedor	**HP**	**XXX**	**XXX-XXX**	**000-0000**	**SI/NO**

Detalle de los recursos de telecomunicaciones

Detalles de la RED LAN

Quito

Configuración Lógica de la Red

Configuración lógica de red Quito

La configuración lógica de las oficinas de Quito utiiza una estructura plana donde todos los dispositivos de red (routers, switches, computadores, impresoras) están en el mismo rango de IP. Dispositivos de red e impresoras usan direcciones de IP estática y los computadores obtienen IP dinámicamente (DHCP server).

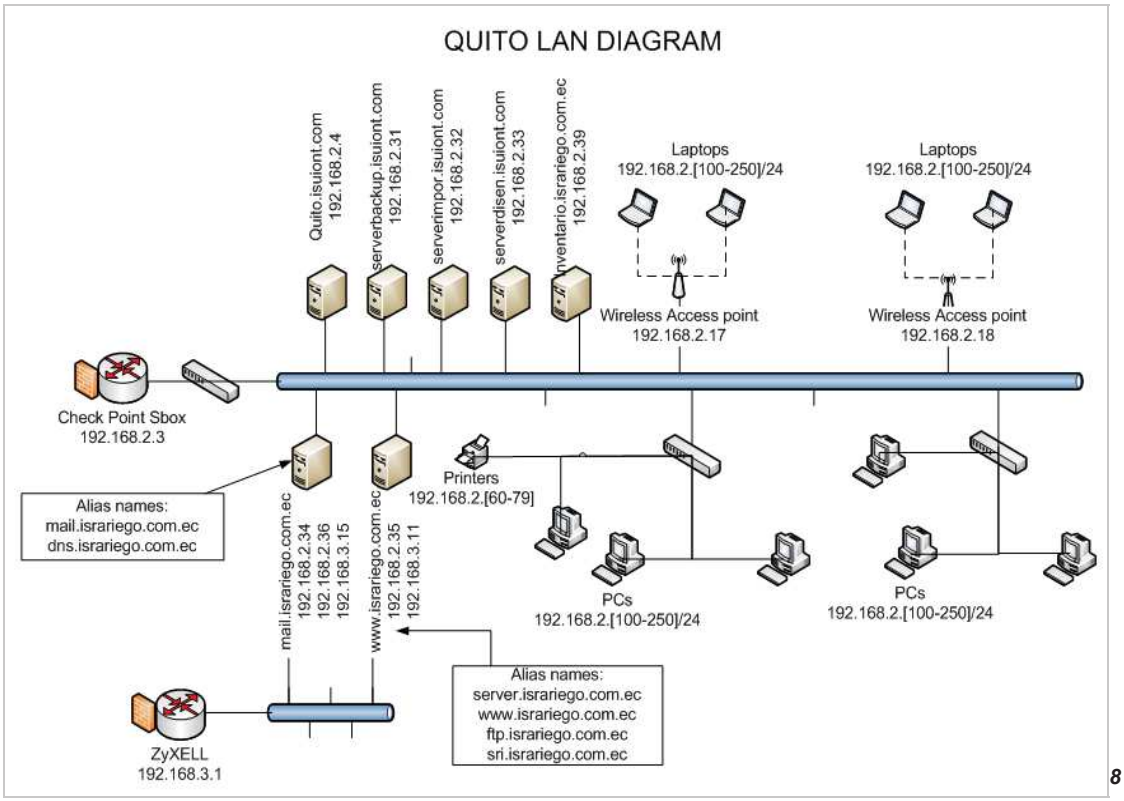
La oficina no tiene core switches y el proceso de ruteo es realizado por los ruteadores.

Designación de direcciones de red IP

Rango de IPs

RANGO IPS	
RANGO	NOMBRE
192.168.[subnet].[1-9]	WAN, VPN and ROUTER devices & Active Directory server
192.168.[subnet].[10-19]	Wireless access point devices
192.168.[subnet].[20-29]	Tests
192.168.[subnet].[30-39]	Servers
192.168.[subnet].[40-59]	Comunicaction devices & other devices
192.168.[subnet].[60-79]	Printers
192.168.[subnet].[80-99]	Free stack
192.168.[subnet].[100-250]	PCs (Asigned by DHCP)
192.168.[subnet].[251-255]	Free stack

Quito		
IP	NOMBRE	ASIGNADA POR
192.168.2.3	Router	Manually
192.168.2.4	Servidor	Manually
192.168.2.17	Wireless access point [No DNS name]	Manually
192.168.2.31	respaldo.isuiont.com	Manually
192.168.2.34	mail.israriego.com.ec	Manually
192.168.2.35	www.israriego.com.ec	Manually
192.168.2.36	dns.israriego.com.ec	Manually
192.168.2.45	VOIP	Manually
192.168.2.66	IMPRESORA_DEPARTAMENTO	Manually
192.168.2.102	Usuario1.isuiont.com	DHCP
192.168.2.107	Usuario2.isuiont.com	DHCP
192.168.2.108	UsuarioLaptop1.isuiont.com	DHCP



8

Quito		
Device	Internal GW	External GW
Sbox	N/a	208.35.122.33
ZyXELL	N/a	208.35.122.41
mail.israriego.com.ec	192.168.3.1	N/a
server.israriego.com.ec	192.168.3.1	N/a
All other servers	192.168.2.3	N/a
PCs	192.168.2.3	N/a
VoIP	192.168.2.3	N/a
Wireless access point devices	N/a	N/a
Printers	N/a	N/a

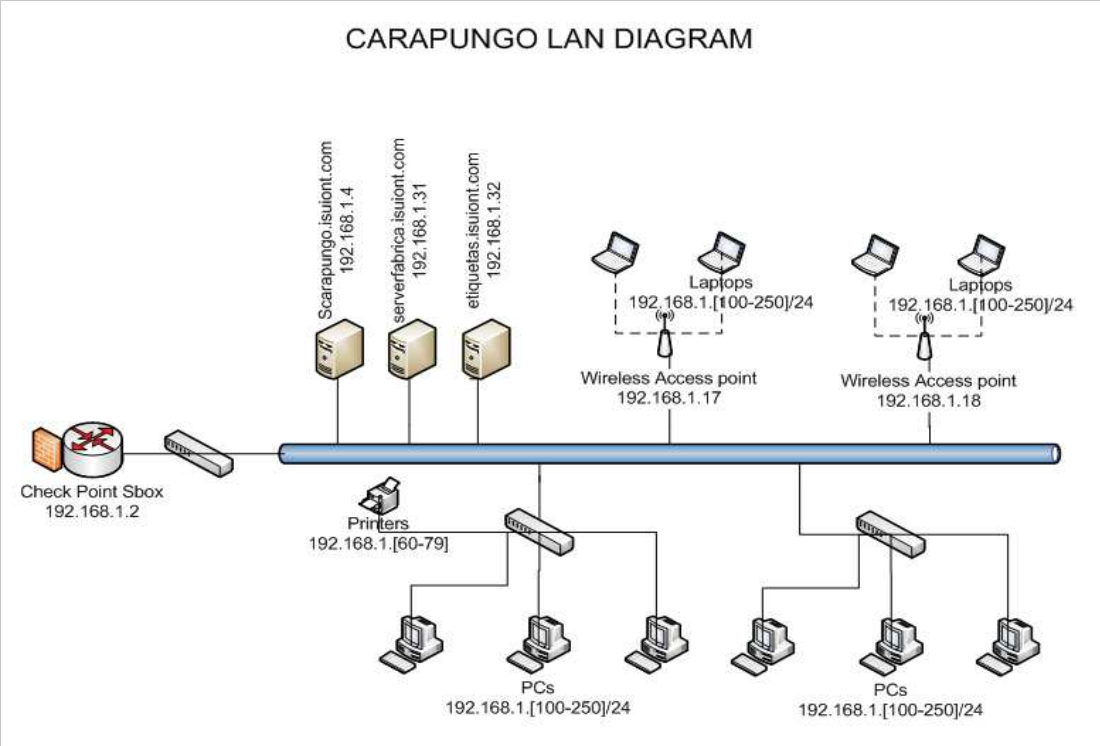
[8] Información enmascara para protección y confidencialidad de Israriego Cia. Ltda.

Carapungo

Rango de Ips

Carapungo		
IP	NOMBRE	ASIGNADA POR
192.168.1.2	Router	Manually
192.168.1.4	scarapungo.isuiont.com	Manually
192.168.1.17	Wireless access point [No DNS name]	Manually
192.168.1.31	servidorfabrica.isuiont.com	Manually
192.168.1.64	IMPRESORA_MANUAL	Manually
192.168.1.101	USUARIO1.isuiont.com	DHCP

Carapungo		
Device	Internal GW	External GW
Servers	192.168.1.2	N/a
Wireless access point devices	N/a	N/a
PCs	192.168.1.2	N/a
Printers	N/a	N/a



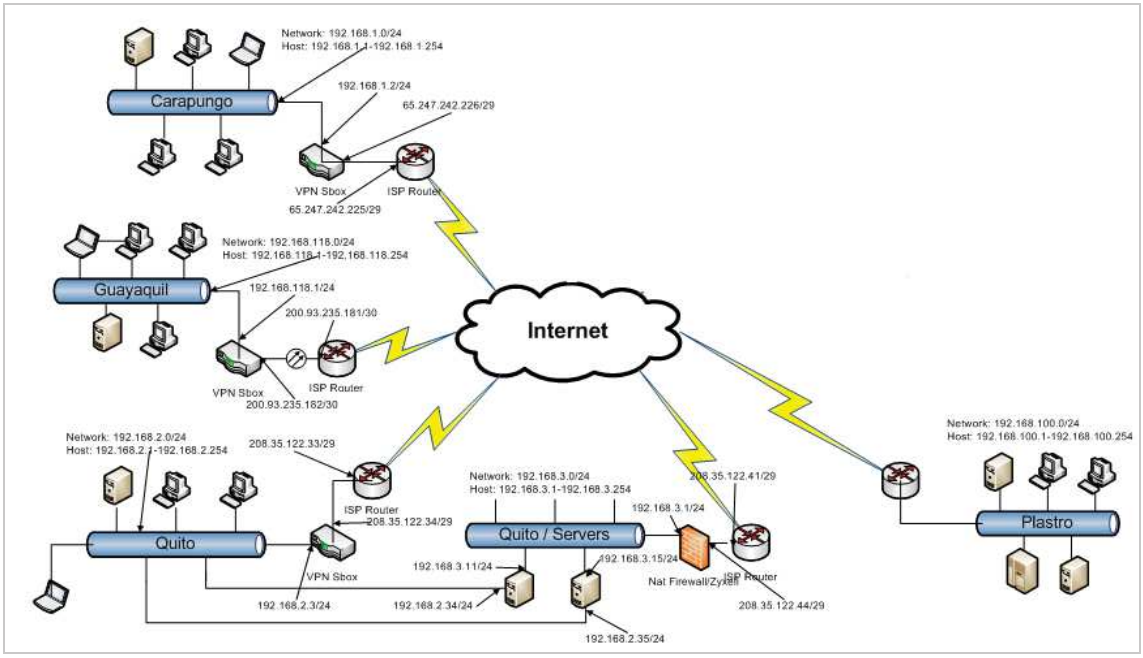
[9]

[9] Información enmascara para protección y confidencialidad de Israriego Cia. Ltda.

Guayaquil

Device	*Internal GW*	*External GW*
Sbox	N/a	200.93.235.181
Servers	192.168.118.1	N/a
Wireless access point devices	N/a	N/a
PCs	192.168.118.1	N/a
Printers	N/a	N/a

Detalles de la RED WAN[10]



[10] Información enmascara para protección y confidencialidad de Israriego Cia. Ltda.

Detalle del equipamiento auxiliar

Detalle del equipamiento

Tipo de equipamiento	Modelo	Ubicación	Nro. Serie
UPS	UPS SMART RT 6000VA 220V	Quito – Sala de Servidores	SNS0935003302
UPS	UPS SMART RT 6000VA 220V	Carapungo – Sala de Servidores	SNS0935003329
UPS	UPS SMART RT 6000VA 220V	Guayaquil – Rack de Servidores Oficina Administrativa	SNS0935003332

Contactos de Soporte

Nombre	Responsabilidad	Contacto	TE Oficina	TE Celular
AKROS CIA. LTDA.	Garantía	Nancy Calle	(593-2) 2-502-334 EXT 222 (593-2) 2-907-676	

Planificación de Contingencias

Evaluación de Riesgos y Prevención

Tan importante como tener un Plan de Recuperación de Desastres, es tomar las medidas para prevenir un desastre o disminuir sus efectos de antemano. Esta porción del plan repasa varias de las amenazas que pueden llevar a un desastre, detalla dónde están nuestras vulnerabilidades, y cuales son los pasos que deberíamos tomar para minimizar nuestro riesgo. Las amenazas cubiertas aquí son causadas por fenómenos naturales y también originadas por el ser humano.

Desastres ambientales

Fuego

La amenaza de fuego en el Data Center, siempre es una posibilidad real y es uno de los factores de riesgo más importante. El edificio está lleno de dispositivos eléctricos y conexiones que podrían recalentar o ponerse en cortocircuito y causar un fuego. A pesar de contar con equipos extinguidores, en lo que se refiere a materiales peligrosos y la ubicación de los equipos, el riesgo es mayor en los horarios en que no hay personal permanente trabajando.

Aunque puede ser rápidamente detectado un principio, el poco tiempo transcurrido puede ser suficiente para afectar seriamente una parte del equipamiento ubicado en este local.

Medidas Preventivas:

Alarmas de fuego: El Data Center debe estar provisto con un sistema de alarma de incendios, con detectores de humo montados en el cielo raso y distribuido a lo largo y ancho del sitio.

Extintores de incendios: Se requieren extintores de incendios portátiles en ubicaciones visibles a lo largo del edificio. El personal debe estar entrenado en el uso de los mismos.

Sistema de Halón: El Data Center debería estar protegido por un sistema de gas Halón que extingue el fuego, minimizando además el daño que este puede producir sobre el equipamiento existente en el lugar.

Recomendaciones:

Deben realizarse revisiones regulares de los procedimientos para asegurar que están actualizados. Las pruebas de extinción de fuego deben ser evaluados por personal experimentado.

También debe realizarse la inspección regular de los equipos de prevención de fuego. La inspección periódica de los extintores de incendios debe formar parte de la política standard.

Erupciones volcánicas

Pueden causar daños significativos a estructura, destruyendo líneas de energía, comunicación, agua, etc. Son posibles los daños estructurales debido a lava o piedras.

Recomendaciones:

Ante el suceso de erupciones volcánicas, el Data Center y las áreas aledañas, deben ser revisadas inmediatamente, sobre todo en los horarios no normales de trabajo (horario nocturno y días no laborables) para permitir la detección temprana de posibles daños producidos por este fenómeno natural.

Temblores de Tierra

Pueden ocurrir daños significativos a estructuras que pueden destruir las líneas de energía y de comunicaciones e interrumpir servicios de agua, gas y otros. También pueden ocurrir daños significativos a la infraestructura incluyendo un colapso total del edificio, puertas, vías de acceso u otras estructuras elevadas.

Recomendaciones:

Ante el suceso de un temblor de tierra, el Data Center y las áreas circundantes, deben ser revisados inmediatamente, sobre todo en los horarios no normales de trabajo (horario nocturno y días no laborables) para permitir la detección temprana de posibles daños producidos por este fenómeno natural.

Incidentes de seguridad

Cyber crimen y sabotaje informático
Pérdida de información (pobres backups o esquemas de recuperación)

Divulgación de información sensitiva

Fallas de sistemas IT

Los incidentes de seguridad están comenzando a ser una amenaza compleja sobre los sistemas y en especial en las instalaciones distribuidas. Con las nuevas tecnologías de gestión de redes, el acceso no autorizado es un riesgo potencial que está presente cada vez en mayor medida.

Este tipo de acciones o riesgos normalmente no afecta el hardware de una manera destructiva. Pueden ser más insidiosos, y pueden venir a menudo desde dentro de la Organización. Un empleado enojado puede construir o ingresar, virus o bombas de acción retardada en las aplicaciones y código de los sistemas. Un empleado bien intencionado puede producir errores que afectan la integridad de los datos (no considerado un crimen, claro, a menos que el empleado haya saboteado programas y datos deliberadamente).

Medidas preventivas:

Todos los sistemas deben tener los productos de seguridad instalados para proteger el ingreso sin autorización. Todos los sistemas deben protegerse por contraseñas, sobre todo las actualizaciones a los datos.

Todos los sistemas deben resguardarse en forma periódica. Esos backups deben guardarse en un área alejada de los datos originales. Debe tenerse especial atención a la criticidad de la seguridad física del área de almacenamiento de datos. Deben establecerse normas sobre el número de ciclos de backups y los tiempos de retención.

Recomendaciones:

Deben mejorarse continuamente las funciones de seguridad en todas las plataformas. Aplicar estrictamente las políticas y procedimientos cuando se descubran violaciones de seguridad.

Mejorar la seguridad de la red: los medios de comunicación compartidos, como la red Ethernet, son susceptibles de actividades de sniffing que los usuarios poco escrupulosos pueden usar para capturar las contraseñas. Lleve a cabo los mecanismos de seguridad más rígidos sobre la red, como las contraseñas por única vez, encriptación de datos y los medios de comunicación no compartidos.

Fallas de los equipos o sistemas:

Falla mayor en un servidor
Falla mayor en la red de datos
Pérdida del Servidor
Pérdida de instalaciones
Falla mayor en el equipo de Aire Acondicionado
Falla mayor en la instalación eléctrica

Medidas preventivas:

Realizar el mantenimiento preventivo de las instalaciones y equipamiento informático, de acuerdo a las recomendaciones de los fabricantes. Definir y poner en práctica normas y políticas para el mantenimiento y la revisión periódica.

Recomendaciones:

Prever la provisión de partes de repuestos y servicio de soporte por parte de los proveedores y fabricantes.

Fallas en servicios públicos o de terceros

Alimentación de energía eléctrica
Red pública de telefonía

Red de Datos WAN

Medidas preventivas:

Poseer equipos de energía eléctrica de emergencia o alternativos (ej. UPS, grupo electrógeno, etc.)

Disponer de equipos de comunicación telefónica inalámbrica (celulares) para comunicaciones de emergencia en caso de la pérdida temporal de la red pública de telefonía.

Recomendaciones:

Realizar pruebas periódicas del funcionamiento y el correspondiente mantenimiento preventivo del equipamiento (equipos de suministro de energía eléctrica, comunicación telefónica).

Estrategia de recuperación

Para facilitar la recuperación de un desastre que destruye todo o parte del Data Center, ciertos preparativos han sido hechos de antemano. Este documento describe lo que se ha hecho para disponer de una rápida y ordenada restauración de las instalaciones del Data Center.

Planificación de la recuperación del desastre

Lo primero y más obvio que hay que hacer es tener un plan. Hasta que punto este plan puede ser eficaz, depende de los planes de recuperación de desastre del resto de los departamentos y áreas dentro de la Organización.

Por ejemplo, si un suceso de desastre afecta al área de informática y a las oficinas del área de Operaciones de Planta, que utiliza la aplicación de "MOVEX", la recuperación completa de la mencionada aplicación puede estar demorada hasta que sea recuperado el normal funcionamiento del área de Operaciones de Planta, aunque el área de sistemas tenga finalizadas sus tareas de recuperación.

Cada área dentro de la Organización debe desarrollar un plan de cómo llevarán adelante sus tareas, en caso de un desastre en su propio edificio u oficinas, o en el caso de un desastre en el Data Center que impiden el acceso a los datos por un período de tiempo. Esas áreas necesitan los medios para funcionar mientras los servicios y aplicaciones de informática no están disponibles, y adicionalmente necesitan un plan para sincronizar los datos que se restauran en los servidores con el estado actual de los mismos. Por ejemplo, si la Oficina de Personal puede registrar los datos nuevos mientras los servidores centrales están fuera de servicio, esos datos tendrán que ser ingresados cuando los servidores vuelven a estar en servicio. Es extremadamente importante que dispongan de los medios para administrar ordenadamente toda la información en forma manual, mientras el servicio de informática no está disponible.

Estrategias de recuperación seleccionadas por Israriego Cia. Ltda.

Israriego Cia. Ltda. ha definido la siguiente alternativa para las 2 situaciones diferentes de desastre.

Situación 1

Pérdida de parte o todo el equipamiento de procesamiento principal (Servidor FQK001 en Guayaquil, FQK002 en Quito y FQQ003 en Carapungo) pero con las instalaciones del Data Center en condiciones de ser usado normalmente:

Es realizado el reemplazo del hardware de procesamiento principal en la misma ubicación física actual del Data Center.

Situación 2

Pérdida de parte o todo el equipamiento de procesamiento principal (Servidor FQK001 en Guayaquil, FQK002 en Quito y FQQ003 en Carapungo), incluyendo las instalaciones del Data Center:

En esta situación es posible hacer la recuperación de los datos a través de la cinta de backup en la unidad de Carapungo, Guayaquil o Quito. Depende cuál unidad fue afectada. Los empleados pueden moverse para la unidad que no fue afectada o trabajar desde su casa con el acceso remoto.

Localización de las unidades:

Quito - Av. Prensa N50-41 y Manuel Valdivieso
Carapungo - El Vergel Lote 19 y Av. Marianitas
Guayaquil - Km 4 ½ Vía Daule y Amadeo Moreira

Sitios alternativos de Recuperación

La Organización ha definido como sitio alternativo de recuperación para el procesamiento de la información de la Unidad de Quito y Guayaquil en la unidad de Carapungo, así también la unidad de Carapungo en la unidad de Quito.

Trabajo del Personal

Las personas que poseen laptop podrán trabajar desde sus casas, hoteles, o cualquier lugar con conexión a Internet si fuera necesario.

Reemplazo del equipamiento

Este plan contiene un inventario completo de cada uno de los servidores, aplicaciones y servicios que deben restaurarse después de un desastre. Los cambios inevitables que ocurren con el tiempo en los sistemas requieren que el plan se actualice periódicamente para reflejar la configuración más actualizada. Para evitar problemas y retrasos en la recuperación, deben realizarse todos los esfuerzos para replicar la configuración actual de la aplicación, servicio o equipo existente. Sin embargo, probablemente habrá casos dónde los componentes no están disponibles o la ventana de tiempo de la entrega es inaceptablemente larga.

El Equipo de Administración de la Recuperación tendrá la especialización y recursos para trabajar a través de estos problemas a medida que ocurran. Aunque algunos cambios pueden requerirse a los procedimientos documentados en el plan, el uso de diferentes modelos de equipos o equipos de diferentes proveedores puede ser conveniente para agilizar el proceso de la recuperación.

Procedimientos de Backup

El hardware necesario puede comprarse. El edificio puede construirse nuevamente. Los empleados pueden contratarse. Pero no pueden comprarse los datos perdidos a cualquier precio. Deben restaurarse de una copia que no fue afectada por el desastre. Hay varias opciones posibles para asegurar que la copia de sus datos sobrevive a un desastre en las instalaciones del Data Center.

La Organización ha seleccionado utilizar en forma rutinaria el “Almacenamiento de los medios magnéticos de Backups fuera del Data Center”, ubicándolo en las unidades de Carapungo, Quito y Guayaquil, con acceso exclusivo para el personal del área de Sistemas, instalada a una distancia prudencial del Data Center.

El backup actual de los datos y aplicaciones varían de acuerdo a la plataforma de hardware sobre el que están instalados. Los procedimientos de backups actualmente vigentes son los siguientes:

Data Recovery Point Objectives (RPO)

Debido al volumen de la información a ser respaldada y a las herramientas de software y hardware disponibles de la Unidad, el RPO para toda la información de la Unidad es: 7 días.

Backup Diario del entorno Windows

Esta unidad ha seleccionado el software de backup **HP Data Protector**, para la ejecución de las tareas de respaldo de datos de todos los servidores Windows.

Las unidades utilizan cintas HP LTO3 Ultrium RW (800GB) para hacer los procesos de backup diario y mensuales.

La política de resguardo de datos definida por Israriego Ecuador es el backup **INCREMENTAL** de datos para todos los procesos diarios, y el backup **FULL** para los mensuales.

Los centros de almacenamiento son:

Quito – Oficina Contabilidad

Las cintas con el backup mensuales de la unidad de Carapungo están almacenados en la cajá fuerte del departamento de Contabilidad

Quito – Oficina Cobranzas

Las cintas con el backup mensuales de la unidad de Guayaquil están almacenados en la cajá fuerte del departamento de Contabilidad

Carapungo – Oficina Gerente Distribuidores

Las cintas con el backup mensuales de la unidad de Quito están almacenados en La cajá fuerte del departamento de Gerencia de Distribuidores

La cinta de limpieza se coloca en el Slot 4, y la limpieza la efectúa automáticamente la unidad de acuerdo a los periodos de lectura/grabación establecidos por el fabricante.

Cada 50 usos, la cinta de limpieza es descartada automáticamente por la unidad, debiendo ser reemplazada por una nueva.

Abajo esta la Politica de backup usado para las unidades de Quito, Carapungo y Guayaquil

Proceso de respaldos

Propósito

Este documento describe el respaldo de servidores de información, especificaciones de respaldos, cronogramas.

Servidores

- Guayaquil
- Quito
- Carapungo

1. Respaldo

Período de retención:
Completo: 40 días;
Incremental: 20 días;
Consolidado: Indefinido.

Especificación de respaldo:

Completo: Todos los datos están copiados;
Incremental: Cinco versiones de cada archivo son cambiadas;
Consolidación mensual: Indefinido;

Frecuencia de respaldo:

Total: Semanalmente;
Incremental: Diariamente;
Consolidación mensual: Mensualmente

Especificaciones	Frecuencia de respaldos			Período de retención
	Diario	Semanal	Mensual	Días
Total		x		40
Incremental	x			20
Consolidación Mensual			N/A	x

2. Plan de respaldos

TOTAL – SEMANALMENTE Y DOMINGOS 12:15AM;
INCREMENTAL – DIARIAMENTE DESDE 12:15AM;

3. Restauración

Cuando el usuario necesite restaurar infomación del respaldo, este debe enviar un mail a IT xxx@xxx.com.

4. Backup housing

Incremental backup tapes are inside the equipment;
Full backup tapes are inside the equipment;

Seguimiento de los procesos de backup

El seguimiento y control de todos los procesos de backup es realizado por el grupo regional de Servidores (RSIS)

Inicio de los procedimientos de emergencia

Listas de notificación

Contactos de emergencia

Detalle	Teléfono	Otros TEL
Seguridad de Planta – Portería	+593 (2) 2822-995 Ext. 111	
Seguridad de Oficina Quito – Portería	+592 (2) 2468-770 Ext 119	
Emergencias – Defensa Civil	911	
Bomberos	102	
Policía	101	
Cruz Roja	131	
Brigada de Explosivos	911	

Lista de notificación primaria del Área Informática

Nombre	Función actual	TEL Interno	TEL particular	TEL móvil

Otros contactos de emergencia

Nombre	Responsabilidad	TEL Interno	TEL particular

Equipos de recuperación de desastres

Para funcionar de una manera eficaz y permitir que las tareas independientes puedan realizarse en forma simultánea, el proceso de recuperación se distribuirá en varios equipos. Este plan requiere de siete equipos que trabajarán juntos, pero que se les asignan porciones específicas de la recuperación.

Los ocho equipos de recuperación de desastres son:

Equipo de administración de la recuperación
Equipo de evaluación de daños
Equipo de recuperación de las instalaciones
Equipo de recuperación de la red
Equipo de recuperación de los servidores
Equipo de operaciones informáticas
Equipo de soporte administrativo

Equipo de Administración de la Recuperación

El Equipo de Administración de la Recuperación es responsable por la coordinación del proyecto completo. Está compuesto de seis personas experimentadas:

Coordinador de la recuperación
Coordinador de las instalaciones
Coordinador técnico
Coordinador administrativo
Coordinador de la red
Coordinador de los servidores

El coordinador de la Recuperación es el líder del Equipo de Administración de la Recuperación y tiene la última autoridad con respecto a las decisiones durante el proceso de recuperación. Cada uno de los individuos restantes será el líder de un equipo especializado que dirigirá una porción de las tareas de la recuperación. Cuando el proceso de recuperación esté en marcha, es probable que exista superposición de áreas o tareas entre los equipos, con lo cual la comunicación interna entre ellos es muy importante. El Equipo de Administración de la Recuperación tendrá reuniones regulares programadas para mantener la comunicación entre los coordinadores de los equipos.

Cada coordinador debe definir anticipadamente una reunión con los miembros de su equipo tan pronto como avancen las primeras actividades planeadas. Una agenda de la primera reunión podría incluir:

- Repaso del estado actual del funcionamiento de la recuperación.
- Revisar las responsabilidades del equipo.
- Confirmar que los miembros están al tanto de cualquier cambio al plan de recuperación original.
- Revisar las tareas asignadas a cada uno de los miembros del equipo.
- Definir el horario y lugar de las próximas reuniones.

Equipo de evaluación de daños

El Equipo de Evaluación de Daños será liderado por el Coordinador Técnico. Él será el responsable de seleccionar a los otros miembros del equipo. Este equipo no será responsable de la evaluación de daños detallada con el fin de ser usada para los seguros contratados. Inicialmente este equipo debe hacer dos cosas:

Proveer información al Equipo de Administración de la Recuperación para poder seleccionar el sitio de la recuperación.

Proporcionar una evaluación de los componentes de hardware recuperables más importantes.

Basado en esta evaluación el Equipo de Administración de la Recuperación puede empezar el proceso de solicitud o adquisición del equipamiento de reemplazo.

Equipo de Recuperación de las Instalaciones

El Equipo de Recuperación de las instalaciones será liderado por el Coordinador de las Instalaciones. Él será el responsable de seleccionar a los otros miembros del equipo.

Este equipo será responsable de supervisar las actividades de reparación y/o reconstrucción del sitio primario (Data Center)

Equipo de recuperación de la red

El Equipo de Recuperación de la red será liderado por el Coordinador de la Red. Él será el responsable de seleccionar a los otros miembros del equipo.

Este equipo será el responsable de supervisar la restauración de la red de datos y comunicaciones de la Organización.

Por ser estos recursos mencionados, uno de los pilares más importantes para el funcionamiento de los servicios y aplicaciones del área de sistemas, debe tener el mayor nivel de criticidad en la restauración.

Equipo de recuperación de los servidores

El Equipo de Recuperación de los servidores será liderado por el Coordinador Técnico. Él será el responsable de seleccionar a los otros miembros del equipo.

La siguiente lista de pasos a seguir por este equipo debe realizarse sobre las diferentes plataformas de hardware existentes:

- Revisión de la evaluación de daños.

- Determinar el hardware, software y repuestos necesarios para iniciar la restauración de cada sistema en particular.

- Comunicar la lista de componentes a ser solicitados o comprados y sus especificaciones al Equipo de Soporte Administrativo.

- Revisar los pasos de recuperación documentados en este plan y realizar cualquier cambio necesario para ajustarlos a la situación actual.

- Cuando el hardware solicitado o comprado comienza a llegar, trabajar con los soporte técnicos contratados o terceras partes responsables de su instalación.

- Cuando todos los componentes están ensamblados, comenzar los pasos de restauración del sistema operativo y datos de los backups existentes.

- Realizar el intento de recrear el estado del sistema al punto inmediato anterior de ocurrido el desastre.

Equipo de operaciones informáticas

El Equipo de Operaciones informáticas será liderado por el Coordinador de Operaciones. Él será el responsable de seleccionar a los otros miembros del equipo.

Este equipo tiene dos funciones principales:

- Proveer asistencia telefónica e información del estado de la recuperación a los usuarios finales.

- Proveer el personal de operaciones para los procesos de las aplicaciones después que los servidores y servicios han sido recuperados.

Equipo de soporte administrativo

El Equipo de Soporte Administrativo será liderado por el Coordinador Administrativo. Él será el responsable de seleccionar a los otros miembros del equipo.

Uno de las funciones más importantes que este equipo tiene es tomar la responsabilidad de las tareas administrativas, para que el personal técnico responsable de la recuperación de los servidores y servicios pueda concentrarse en su tarea específica.

La siguiente es un detalle inicial de sus tareas:

Proveer soporte para la ejecución de las compras

Brindar asistencia en las tareas de evaluación de daños y garantizar los procedimientos administrativos de la organización.

Determinar el estado del personal que estaba trabajando al momento del desastre.

Proveer el contacto y apoyo al personal y miembros de las familias, afectado por el desastre.

Asistir a los Coordinadores de Equipo para la ubicación de los potenciales miembros de cada equipo.

Coordinar los arreglos requeridos para la provisión de la comida y descanso necesarios del personal de recuperación.

Proveer soporte para el registro de los gastos relacionados con el desastre

Proveer soporte en las relaciones públicas.

Proveer apoyo de contacto con las terceras partes involucradas en las tareas de recuperación o entrega de equipamiento, suministros y demás necesidades externas)

Detalle Equipos de Recuperación

Equipo	Cargo	Nombre	Apellido	Teléfono
Administración de la Recuperación	Coordinador de la Recuperación			
	Coordinador de la Recuperación (alternativo)			
Evaluación de Daños	Coordinador técnico			
	Coordinador técnico (alternativo)			
Recuperación de las instalaciones	Coordinador de las instalaciones			
	Coordinador de las instalaciones (alternativo)			
Recuperación de la Red	Coordinador de la red			
	Coordinador de la red (alternativo)			
Recuperación de los Servidores	Coordinador Técnico			
	Coordinador Técnico (alternativo)			
	Coordinador de las aplicaciones (alternativo)			
Operaciones Informáticas	Coordinador de Operaciones			
	Coordinador de Operaciones (alternativo)			
Soporte Administrativo	Coordinador administrativo			
	Coordinador administrativo (alternativo)			

Activación del Plan de Recuperación de desastres

Designación del coordinador de la recuperación

El primer objetivo es definir al Coordinador de Recuperación. La persona más apropiada para esta función es la persona que tiene el mejor conocimiento de la unidad. Si esta persona no está disponible, la designación debe ser una persona del grupo regional de TI. Esta persona debe tener experiencia en la administración del Data Center y debe tener la autorización de la firma para los gastos necesarios durante el proceso de la recuperación. Revisar “Equipos de Recuperación de Desastre” para consultar las responsabilidades del Coordinador de la Recuperación y la lista sugerida de las personas que pueden llenar este y otros roles de coordinación.

Determinación del status del personal

Una de las primeras tareas importantes del coordinador de Recuperación es determinar el estado del personal que trabajaba en el momento del desastre. El personal de seguridad en el sitio después del desastre efectuará cualquier rescate o primeros auxilios necesarios a las personas alcanzadas por el desastre. Sin embargo, el coordinador de la Recuperación debe generar una lista de las personas que estarán disponibles para ayudar en el proceso de recuperación.

El coordinador de la Recuperación también debe definir rápidamente al Coordinador de Soporte Administrativo cuya responsabilidad será identificar a cualquier persona herida o lastimada por el desastre. El Coordinador de Soporte Administrativo trabajará con las familias y empleados, atendiendo sus necesidades.

Tomar el cuidado de nuestro personal es una tarea muy importante y debe recibir la prioridad más alta, inmediatamente después del desastre. Mientras

tenemos una tarea técnica enorme por delante para restaurar los servidores y servicios informáticos, no podemos perder de vista los intereses de las personas afectadas por el desastre.

Protección y rescate del equipamiento y medios magnéticos

Un objetivo primario del proceso de recuperación es restaurar todos los servidores y servicios sin la pérdida de datos. Es importante que el coordinador de la Recuperación defina al Coordinador Técnico rápidamente para que él pueda ponerse inmediatamente sobre la tarea de proteger y salvar cualquier medio magnético de almacenamiento de datos. Esto incluye cualquier cinta magnética, discos ópticos, CD-ROM y unidades de disco.

Establecimiento del Centro de Control de la recuperación

El Centro de Control de la Recuperación es el lugar desde el cual es coordinado el proceso de recuperación de desastres. El coordinador de la Recuperación debe designar donde será establecido el Centro de Control de la Recuperación.

Activación del plan de recuperación de desastre

El coordinador de la Recuperación pone el plan en ejecución. Los pasos iniciales a tomar son los siguientes:

El coordinador de la Recuperación debe obtener una copia actualizada de este Plan de Recuperación de Desastres resguardada en la caja fuerte de contabilidad en las oficinas de Quito. Este plan debe estar impreso en papel y también disponible en medio magnético (disquete o CD-ROM). Deben hacerse copias del plan y deben entregarse en la primera reunión del Equipo de Administración de la Recuperación.

El coordinador de la Recuperación determina los restantes miembros del Equipo de Administración de la Recuperación. Esto debe hacerse en una deliberación con los miembros disponibles del personal de Sistemas y el personal auxiliar de la Planta, y con la aprobación del Personal jerárquico inmediato superior. La decisión del coordinador de la Recuperación sobre quién forma parte del Equipo de Administración de la Recuperación debe respetarse como la definitiva.

El coordinador de la Recuperación debe llamar a una reunión del Equipo de Administración de la Recuperación al Centro de Control de la Recuperación o a un sitio alternativo designado. La persona con mayor nivel de la organización que está presente en este momento, debe ser invitado a esta reunión. La siguiente agenda es sugerida para esta reunión:

Cada miembro del equipo debe revisar el estado actual de sus áreas respectivas de responsabilidad.

Después de esta revisión, el coordinador de la Recuperación toma la última decisión sobre dónde hacer la recuperación. Si una ubicación determinada de la Organización es seleccionada como sitio alternativo, el coordinador de la Recuperación declarará el uso de emergencia de esa instalación y notifica a la persona con mayor nivel jerárquico de la Organización presente.

El coordinador de la Recuperación revisa brevemente el Plan de Recuperación de Desastre con el equipo.

Cualquier ajuste al Plan de Recuperación de Desastre para adaptarse a las circunstancias actuales será discutido y definido.

Cada miembro del equipo es puesto a cargo de su papel respectivo en la recuperación y comienza con el trabajo definido en el Plan.

Cada miembro del equipo revisa la composición de sus equipos de recuperación respectivos. Si los individuos claves de uno de los equipos de recuperación no están disponibles, el coordinaodr de la Recuperación debe ayudar en la ubicación de otras personas que tengan las habilidades y experiencia necesarias, incluyendo la ayuda externa de otras áreas de Sistemas o proveedores de soporte.

La próxima reunión del Equipo de Administración de la Recuperación es definida. Se sugiere la reunión del equipo por lo menos una vez por día durante la primera semana del proceso de la recuperación.

Los miembros del Equipo de Administración de la Recuperación comienzan el proceso de avisar a las personas que formarán parte de sus respectivos equipos de recuperación y llamarán a las reuniones para poner en marcha inmediatamente su parte de la recuperación.

La persona con mayor nivel jerárquico de la Organización presente, es responsable de que esté disponible en forma inmediata el Centro de Control de la Recuperación, para que pueda ocuparlo el Equipo de Administración de la Recuperación. Esto incluye la reubicación inmediata del personal que ocupa ese lugar. Además, debe ayudar al Coordinador Administrativo para ubicar los recursos básicos para el Centro de Control:

- Escritorios y sillas
- Teléfonos
- Computadoras personales
- Impresoras
- Equipo fax
- Fotocopiadora

Las comunicaciones móviles serán importantes durante las fases iniciales del proceso de recuperación. Esta necesidad puede satisfacerse mediante del uso de teléfonos celulares y/o equipos de radiofrecuencia.

Protección y recuperación del equipamiento

Este documento contiene información sobre los procedimientos a ser usados inmediatamente después de un incidente, para preservar y proteger los recursos en el área dañada.

Protección

Es extremadamente importante que cualquier equipamiento, medio magnético, stock de papeles y otros elementos en el sitio primario dañado sean protegidos, para evitar cualquier extensión del daño. Alguno de estos elementos pueden ser recuperables o reparables en operaciones de restauración.

Reunir todos los cartuchos de cinta magnética en un lugar determinado y rápidamente cubrirlos con una lona o plástico para evitar el daño del agua.

Cubra todo el equipamiento informático para evitar el daño del agua.

Cubra el stock de papeles para evitar el daño del agua.

Solicite al personal de Seguridad de la Planta o al personal Policial, que ubique una guardia de seguridad en el sitio primario (Data Center) para prevenir que personas ajenas al sector entren al lugar o extraigan equipos o materiales sin autorización.

Rescate de medios magnéticos y ópticos

Los medios magnéticos y ópticos en los cuales están almacenados nuestros datos son inapreciables. Aunque poseemos backups de nuestros subsistemas de discos y datos fuera del sitio primario (Data Center), las cintas magnéticas almacenadas en este lugar contienen información sumamente valiosa y que sería muy importante no perder. Si los medios magnéticos han sido destruidos,

por ejemplo a causa del fuego, nada puede hacerse. Sin embargo, el daño provocado por el agua y el humo puede a menudo revertirse, por lo menos para permitir copiar los datos.

Después de proteger los medios magnéticos y ópticos de la extensión del daño, la recuperación debe empezar inmediatamente para evitar la pérdida total. Existen empresas especializadas en la recuperación de datos almacenados en medios magnéticos y ópticos dañados.

Rescate del equipamiento

Tan rápido como sea posible, todo el equipamiento y suministros recuperables deben ser trasladados a una ubicación segura. El transporte debe ser organizado por el coordinador de la Recuperación para mover el equipamiento y suministros a un área segura (como un depósito)

Si el equipamiento ha sido dañado, pero puede ser reparado o restaurado, es recomendable trasladarlos a una ubicación alternativa dónde puedan secarse y ser reparados.

Inventario

Cuando sea posible y práctico, debe tomarse un inventario completo de todo el equipamiento recuperable, junto con las estimaciones sobre cuando los equipos estarán listos para su uso (en el caso que una reparación o restauración sea necesaria). Este inventario debe entregarse al Coordinador Técnico y al Coordinador Administrativo, quienes lo usarán para determinar qué elementos del equipamiento y suministros deben obtenerse o comprarse para comenzar la recuperación de los sistemas.

Evaluación de daños

Esta evaluación de daños es un intento preliminar para establecer la magnitud del daño al hardware crítico y las instalaciones donde están ubicados. El objetivo primario es determinar donde la recuperación debe tomar lugar y qué hardware es necesario pedir inmediatamente.

Los miembros del equipo deben ser libres en su estimación del tiempo requerido para reparar o reemplazar un recurso dañado. Tenga en cuenta los casos en dónde una reparación no puede empezar hasta que otro paso ha sido completado. Las estimaciones del tiempo de la reparación deben incluir el pedido, envío, instalación y tiempo de prueba.

Para generar una lista con la evaluación de daños del hardware, debe tomarse como base la lista original, detallada en este documento. La mencionada lista contiene el equipamiento crítico necesario para una recuperación total de los servicios.

Va a ser necesario separar los elementos en dos grupos. EL primer grupo incluirá los elementos perdidos o destruidos. El segundo grupo incluirá aquellos elementos considerados recuperables. Estos elementos recuperables tendrán que ser evaluados por personal técnico y reparados si es necesario. Basándose en esta secuencia de pasos, el equipo de Administración de la Recuperación puede empezar el proceso de adquisición de los reemplazos necesarios.

Con respecto a las instalaciones, la evaluación de daños a la estructura debe revisar el sistema eléctrico, el aire acondicionado, y la red de datos y comunicaciones.

Procedimientos de Compras de emergencia

El Coordinador de Soporte Administrativo es el responsable de todas las compras de emergencia para el área de Sistemas. Todos los miembros del Equipo de Recuperación de Desastres deben dirigir sus requerimientos al Coordinador.

El Coordinador seguirá las normas y políticas establecidas para la compra de emergencia y trabajará con el Comprador que ha sido designado por la Oficina de Compras para completar la adquisición. Si la Oficina de Compras ha sido afectada severamente por el desastre y no puede funcionar normalmente, el Coordinador realizará directamente todas las tareas del ciclo de compras necesarias.

El Coordinador de Soporte Administrativo también es responsable de realizar el seguimiento de todas las compras, el resguardo de los registros financieros del proceso de recuperación de desastres y de controlar que todos los procedimientos de compras pasarán la revisión de la auditoria (interna o externa).

Procedimientos de inicio de la recuperación

Procedimientos de recuperación de la plataforma de Hardware y Software (Windows)

1. Alcance

Esta instrucción de trabajo tiene por objetivo documentar todo el proceso de restauración de servidores Windows 2003

2. Propósito

Describir de manera clara y concisa todas las etapas necesarias para restaurar un servidor en caso de que sea necesario.

3. Responsables

Administrador de Servidores

4. Procedimiento

- Para el proceso de restauración de un servidor serán necesarios:
- CD con Imagen;
- Cintas con copia de datos para restauración
- Cintas con librerías

1ª Fase - Restaurando el Sistema Operacional:

1. Inserte el disquete de arranque en la unidad de CD, así como con el estándar de la imagen;

2. Reinicie el servidor. Asegúrese de que el sistema operativo está configurado para Windows2000/2003;

3. Pulse la barra espaciadora cuando vea la señal de "arranque"; particionar sus discos seleccione la opción "inicio limpio - No hay controladores".

4. Seleccione "Repart Todos", para usar todo el disco como partición de arranque primero;

5. Reinicie el servidor;

6. Pulse la barra espaciadora cuando vea la señal de "arranque", esta vez seleccione Crear - Crear CD-ROM;

7. Ingrese la información correspondiente y presione "OK";

8. Una vez completado el paso anterior, inicie el proceso de Build.exe. Seleccione el menú usando las teclas de flecha, la versión del sistema operativo que se está construyendo y presionar "Enter" - de advertencia, podrían ser listados diferentes versiones del sistema operativo;

9. El proceso tomará de 20 a 40 minutos, el proceso de formateo se realiza automáticamente. Usted no debe recibir ninguna pantalla o mensaje de error;

10. Después de esto, vaya al servidor para asegurarse de que todo está funcionando correctamente en el entorno del sistema operativo.

2ª Fase - Instalando el cliente de Sistema de Backup:

1. En la pantalla principal del Data Protector, selecione el menu “Clients”, conforme la figura 1 abajo:

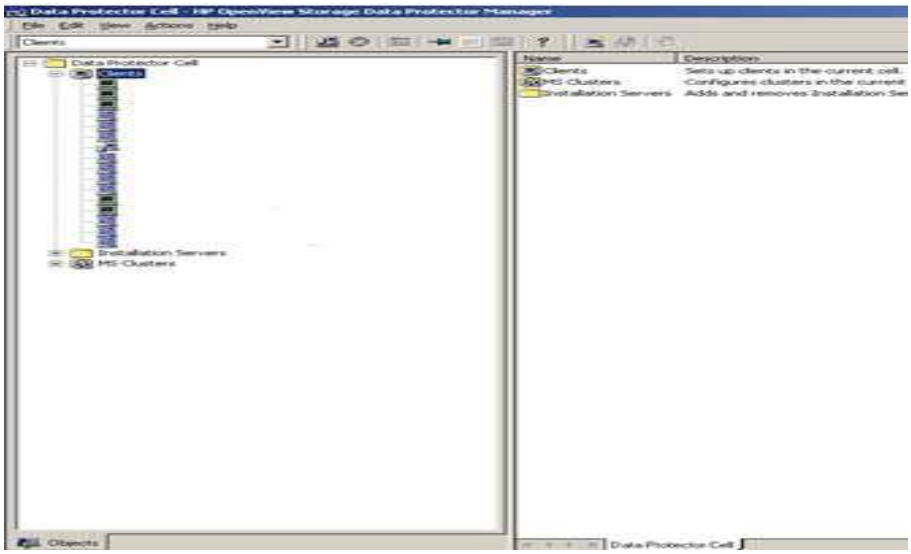


Figura 2

2. Dé click en el botón directo del mouse de selección u opción “Add Clients”, conforme la figura 2 abajo:

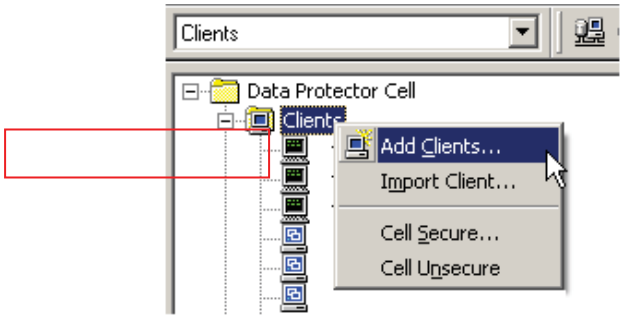


Figura 3

3. Después de efectuado el paso 2, la siguiente pantalla será mostrada, ver figura 3 abajo

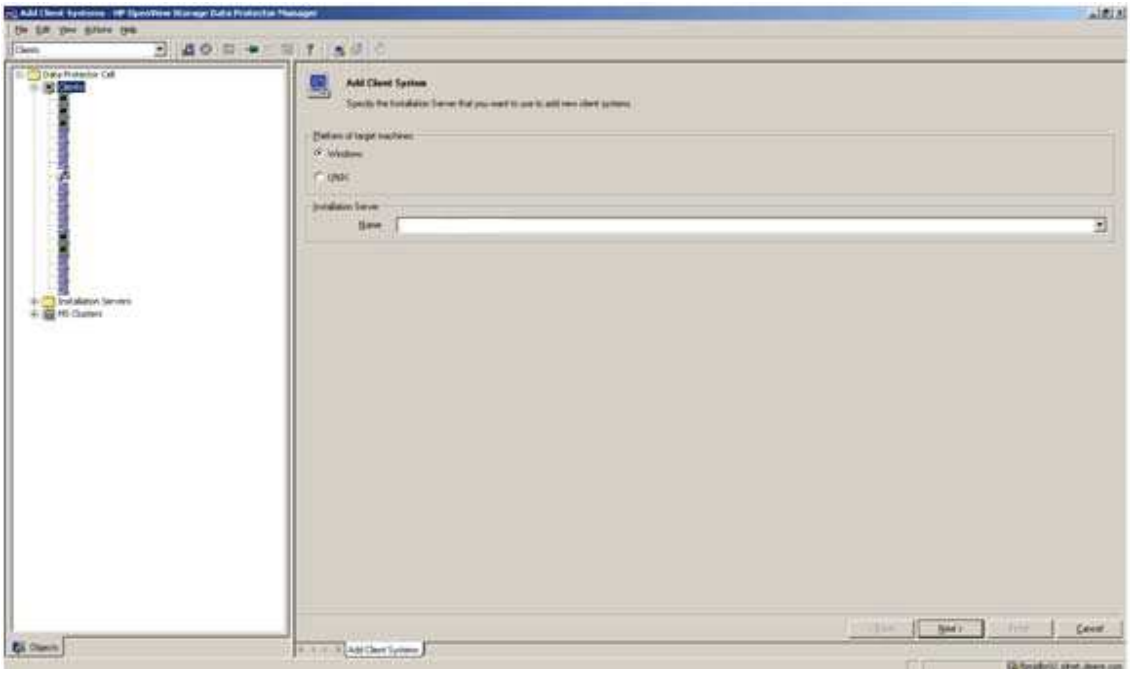


Figura 4

4. Seleccione el Sistema Operacional acorde a la necesidad:

Ambiente Windows

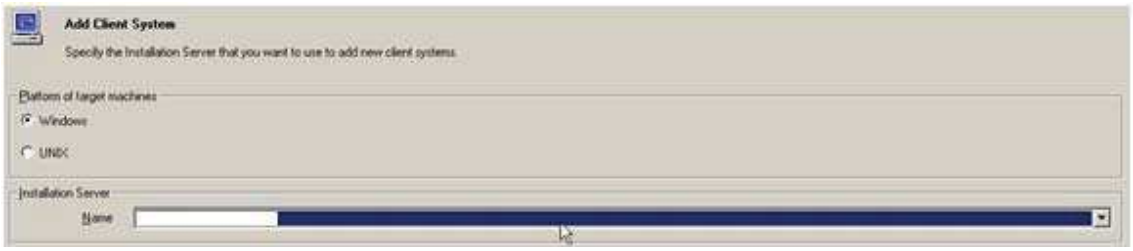


Figura 5

5. Después de seleccionado el Sistema Operacional, digite el nombre del cliente que será adicionado, ver figura 5:

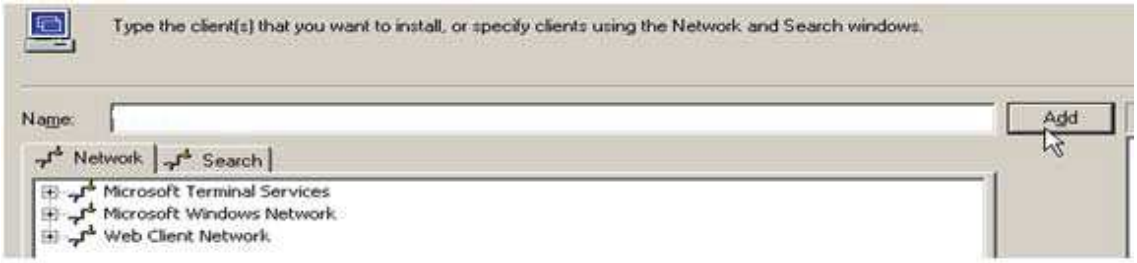


Figura 6

6. Agregado el cliente, en la siguiente pantalla agregar la función necesaria, en este caso seleccione “Disk Agent”

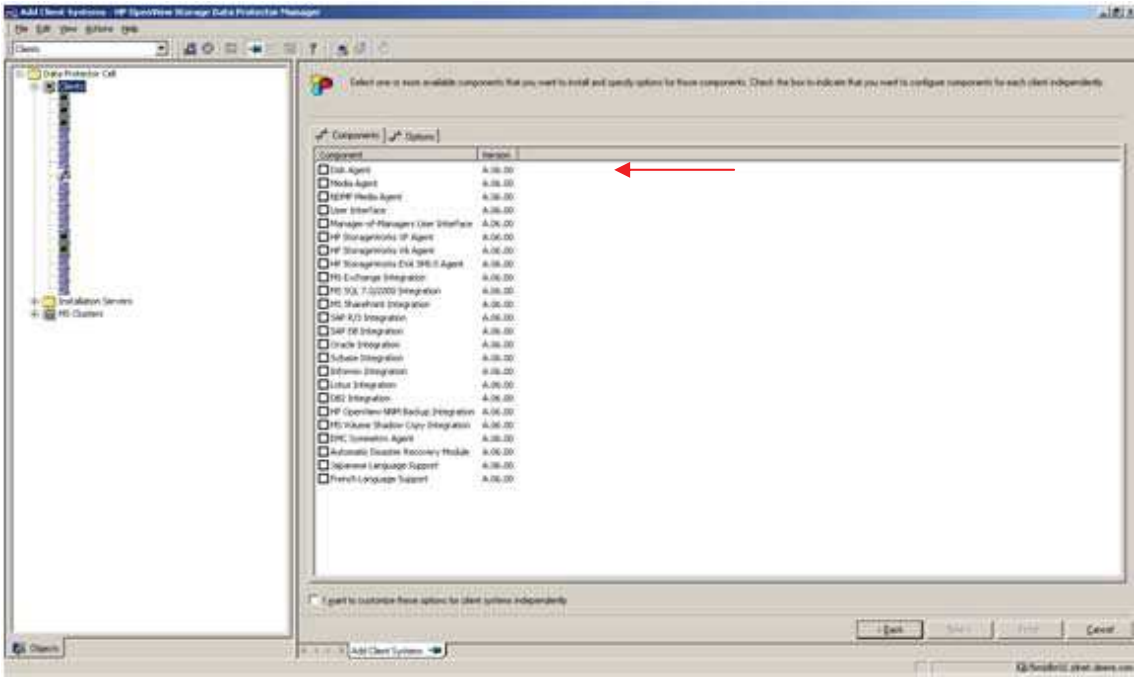


Figura 7

3ª Fase – Restauración de datos:

1. En la pantalla principal del Data Protector, seleccione el menú “Restore”, ver figura 8 abajo:

Figura 8

2. Busque el servidor deseado dentro de las carpetas:

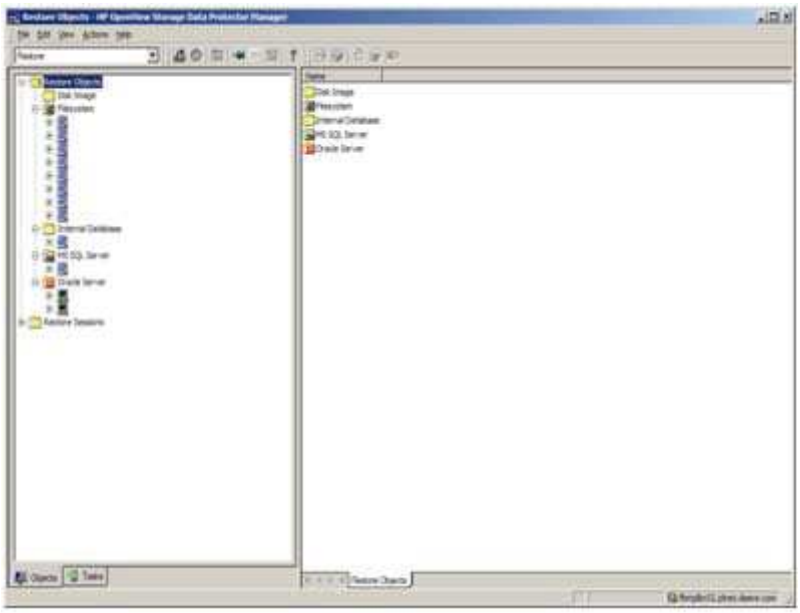


Figura 9

3. Después de seleccionado el servidor, seleccione el disco que se necesita restaurar, conforme a lo indicado en la figura 10:

- Nota: Si fuese necesario restaurar solamente una única partición no seleccione todo, ya que esto le ahorrará tiempo.

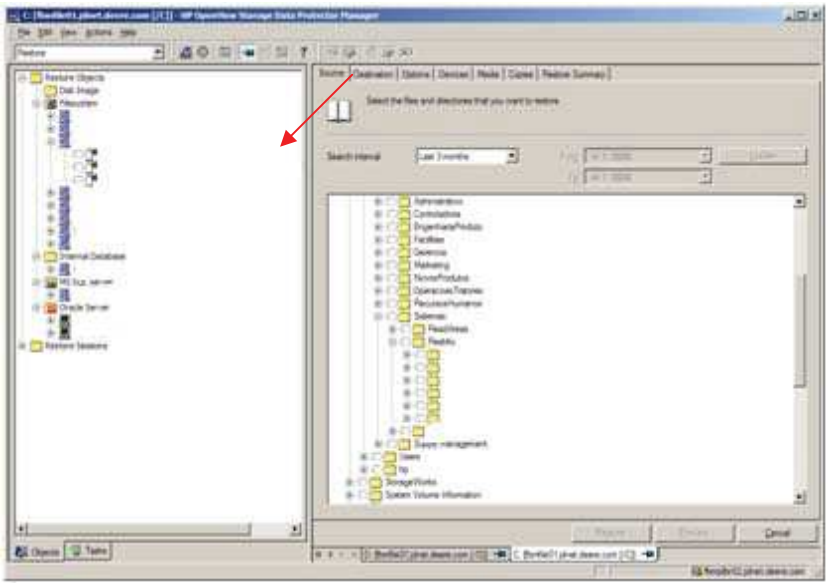


Figura 10

3.1 Por padrón del sistema automaticamente se cargará la última versión copiada, como en este caso sera necesario versiones mas antiguas, usted debe seleccionar el archivo/directorio/disco y con click derecho escoger la opción “Restore versión” como se ve en la figura 11:

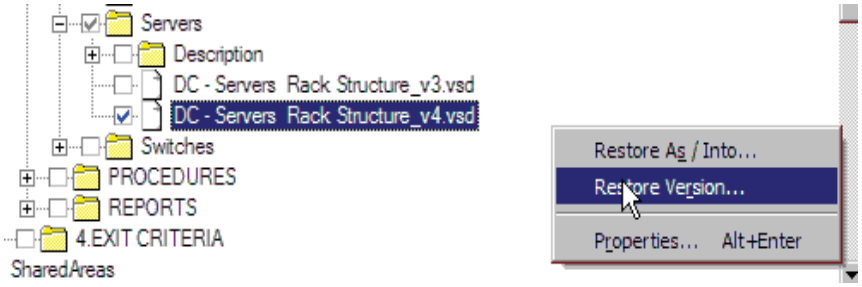


Figura 11

4. La siguiente ventana se abrirá, seleccione la opción “Backup Version”, seleccione la versión deseada como se muestra en la figura 12

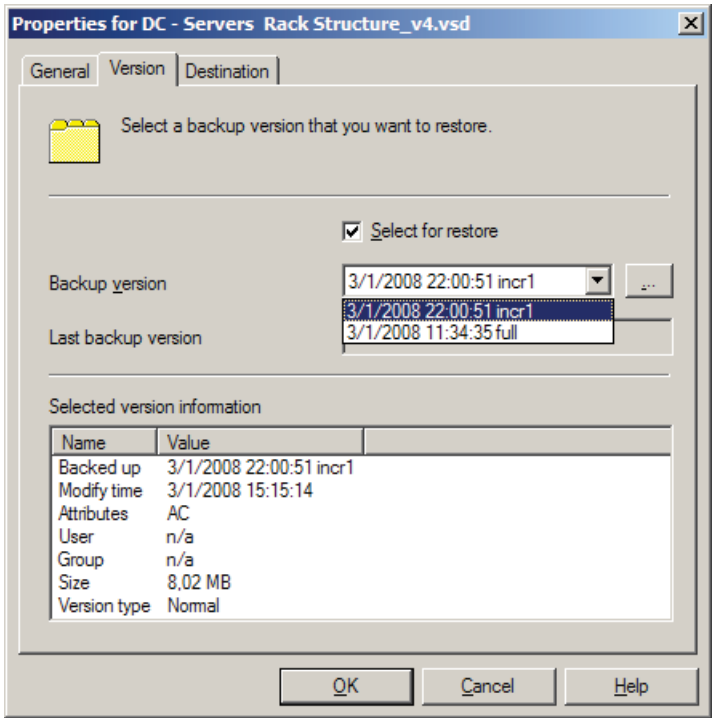


Figura 12

5. Completada la etapa anterior, ahora usted debe seleccionar “Destination”, conforme la figura 12:

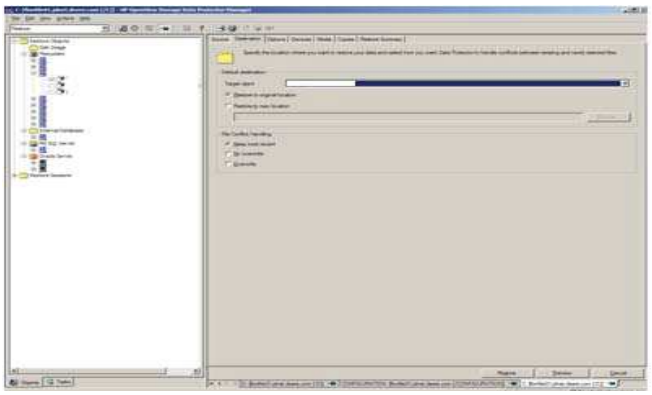


Figura 13

6. Seleccionar la opción “Overwrite” conforme la figura 13:

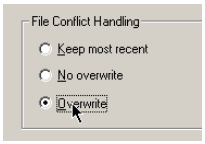


Figura 14

7. Escoger en el menú “Option” la opción indicada en la figura 14

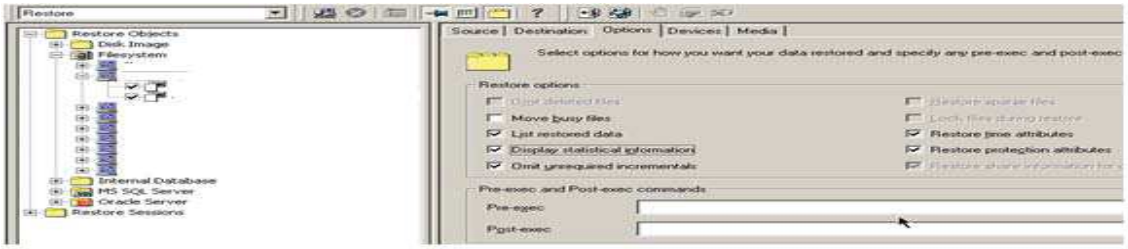


Figura 15

8. Escoger la opción “Restore”, en la pantalla seleccionar la forma de restauración de los objetos. Seleccione “All objects (paralell restore)” y dar click en siguiente, ver figura 15:

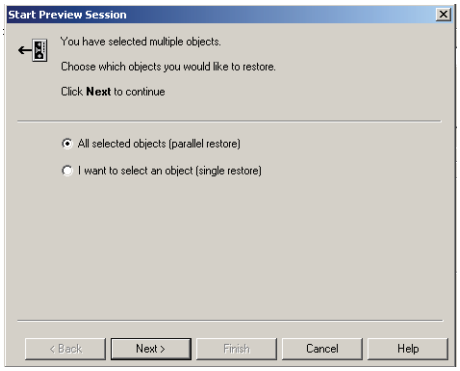


Figura 16

9. Escoger botón “finish”:

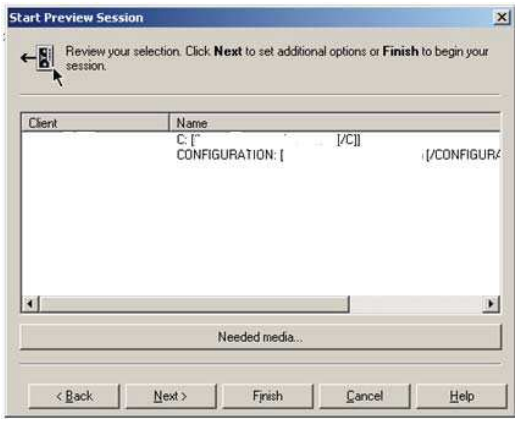


Figura 17

10. Esperar que todos los datos sean restaurados y luego reiniciar el servidor.

4ª Fase – Verificación de restauración:

Luego que el proceso “reboot” sea ejecutado, todo el ambiente debe ser revisado para garantizar el funcionamiento correcto.

Los principales ítems a verificar son:

1. Identificar IP – Validar que la dirección IP este correctamente asignado al equipo.

En el menú iniciar, revisar en “Network Connections” (Start> Settings> Network Connections);

Seleccione el adaptador de red:

Figura 18

2. Click derecho seleccionar la opción “Properties”:

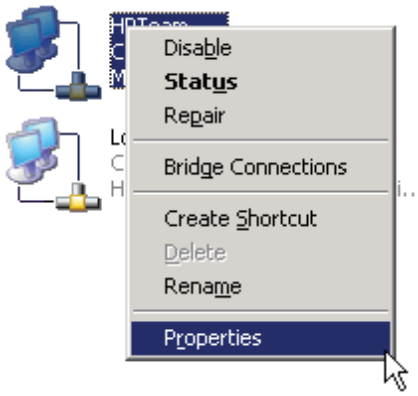


Figura 19

3. En la pantalla de configuración de TCP/IP, insertar la información necesaria en los siguientes campos:

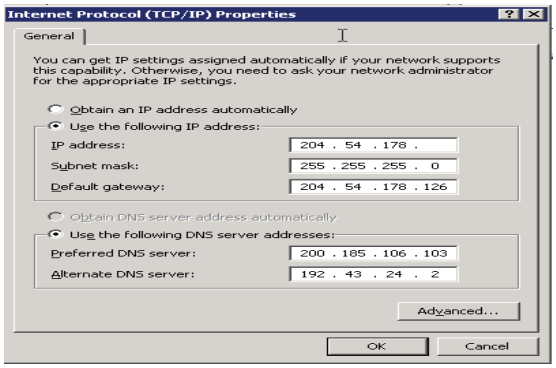


Figura 20

4. Dar click en ok luego de ingresar los datos.

5. Autenticación de Dominio – Certificar que el equipo logra ser visualizado y visualizar los demás dispositivos de red.

6. En el menú inicial escoger la opción RUN, y digite el nombre de cualquier servidor que tenga servicios compartidos, ver figura 20:

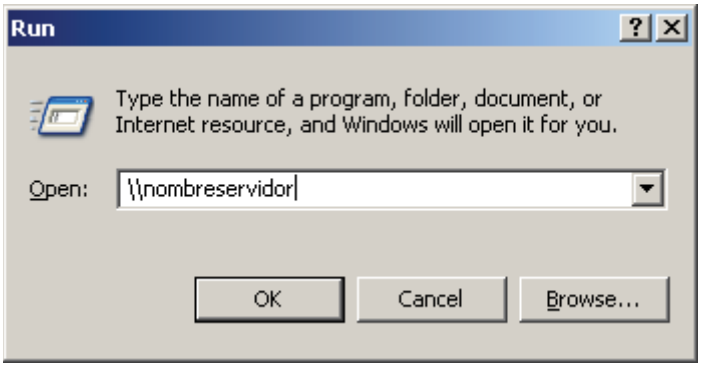


Figura 21

7. El resultado debe ser una pantalla de Explorer mostrando las carpetas compartidas.

8. En caso de error deberá sacar el servidor del dominio e ingresarlo nuevamente.

9. Después de realizar todas las verificaciones anteriores, debe analizar posibles problemas o conflictos que surjan.

10. En el caso de que ningún problema sea detectado, reiniciar las aplicaciones relacionadas con el equipo y dejar que los usuarios accedan.

Escrito por:	**Revisado por:**	**Aprobado por:**
Nombre **Cargo**	**Nombre** **Cargo**	**Nombre** **Cargo**

La estructura de los servidores en las unidades de Quito, Carapungo y Guayaquil se considera como datos confidenciales.

Procedimientos de recuperación de las telecomunicaciones

El procedimiento de recuperación para todos los recursos que componen las telecomunicaciones se realizara mediante la coordinación con el proveedor correspondiente. Básicamente, ante la aparición de un problema o la necesidad de recuperar alguno de estos recursos, el proveedor cuyos contactos se encuentran en la lista de contactos, será llamado por el equipo de recuperación de la infraestructura.

Proceso de recuperación de Acceso a Centro de Datos

Objetivo

Definir niveles de acceso al cuarto de servidores de las instalaciones de Fábrica ubicadas en XXXXX y diferentes modos de acceso.

Servidores/equipos involucrados

Servidor principal de datos y servicios de DHCP, Servidor de impresiones
Servidor SMS

Recuperación

El acceso al cuarto de servidores comparte un acceso principal con la oficina del gerente de RRHH, las llaves del acceso principal al departamento de RRHH y del cuarto de servidores están bajo el poder del Gerente de Planta en la caja de almacenamiento.

De ser necesario y para agilitar labores administrativas, el custodio de la caja o armario general de llaves podrá delegar el cuidado de las llaves a un empleado a su cargo (Conserje).

Adicionalmente el personal del departamento de IT posee llaves el cuarto de servidores, así como también reposan las llaves del cuarto de servidores en el departamento de IT – Oficinas Quito, estas se encuentran en el cajón del escritorio del Analista de IT.

Contactos

- Nombre:
- Cargo:
- Teléfono:

Proceso de recuperación de UPS y Aire Acondicionado

Objetivo

Establecer el procedimiento en una situación de contingencia por la falta de energía.

Equipos involucrados

UPS Cuarto de Servidores Quito, Carapungo y Guayaquil
Aire Acondicionado de Cuarto de servidores de Quito y Guayaquil

Recuperación

UPS

En caso de ocurrir falla en el equipo de UPS del cuarto de servidores, se realizará cambio de cables de conexión de los equipos de: 2 Servidores, 1 backup, 1 router, 1 switch, se utilizarán los cables de conexión directa a la energía utilizando el tipo de "**enchufe Tipo B".**

Una vez reestablecidas las conexiones de servidores, se realizará el reclamo por garantía del equipo al proveedor detallado en la planilla.

Aire Acondicionado

En caso de existir fala en el equipamiento de aire acondicionado usado en la sala de los servidores se realizará contacto inmediato con el proveedor de mantenimiento para solución de fallo.

Contactos

- Nombre:
- Cargo:
- Teléfono:

Proceso de recuperación de sistema de impresiones

Objetivo

Establecer el procedimiento en una situación de contingencia por falla en el sistema de Impresiones

Equipos involucrados

Servidores de cuarto de Servidores Quito, Carapungo y Guayaquil

Recuperación

Para la instalación del software de impresiones MOM es necesario:

CD de Software de Instalación MOM

Cintas con información de Datos Impresoras

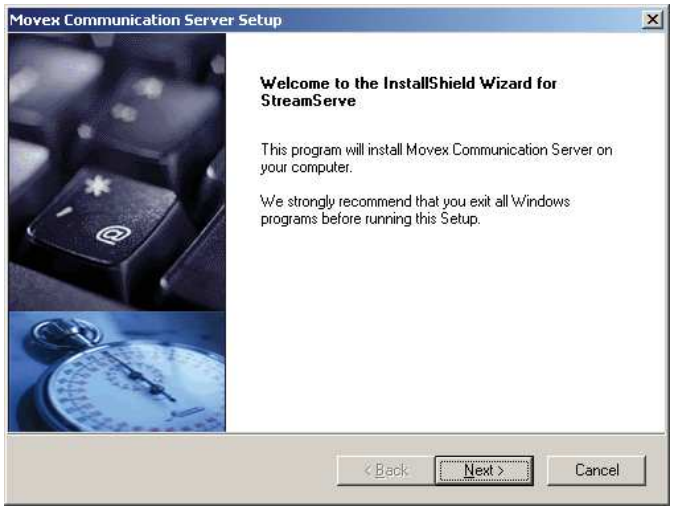
INSTALACIÓN SOFWARE MOM

1.- Ingrese el disco de instalación del programa MOM.

2.- Se abre la pantalla que se ve así:

3.- Presionar en Movex Communication Server.

4.- Se abre la siguiente pantalla:



5.- Presionar NEXT en todas las pantallas siguientes hasta FINISH.

6.- NO reiniciar el equipo

7.- Presionar Movex Tools.

8.- Presionar NEXT en todas las pantallas hasta el final.
9.- De la misma forma instalar Forms Design y Movex Output Implementation.
10.- Presionar EXIT y salir del menú principal.
11.- Abrir MY COMPUTER y hacer Browse en el CD.
12.- Copiar las carpetas strs.exe y strsvc.exe en el archivo to_program files hacia el archivo C:\Program files \StreamServe\3.0\Server.
13.- Copiar las carpetas Services del disco al archivo C:\MVXOUT.
14.- Copiar el archivo DUX que esta en \\mom\mvxout\services\common hacia c:\mvxout\services\common.
15.- Copiar el archivo Translation.sls que esta en \\mom\mvxout\services hacia c:\mvxout\services\common.
16.- Copiar el archivo ServidorOrigen que esta en \\mom\mvxout\services hacia C:\mvxout\services\servidor
17.- Reiniciar equipo.
18.- Borrar el atajo en la mesa de trabajo: Mvxout3
19.- Crear un nuevo atajo al Process Manager.
20.- Bajar la opción Read only del archivo MVXOut y explorer 113.
21.- Abrir el archivo PlatformStreamServer.dpp que esta en C:\mvxout\services\servidor

Dentro del archivo abrir TCP_Movex y cambiar la IP bajo la pestaña de Settings a la dirección del software adecuado. Verificar que el número de puerto sea 20102.

Observación: Si existe mas de 1 StreamServe adelantar los puertos en una unidad cada vez.

22.- Hacer Export y Save y aparecen 2 señales de error, aceptar y salir.
23.- Iniciar el Process manager.
24.- Señalar los Servicios. Al lado derecho hay definiciones que se deben cambiar:

- Cambiar Working Directory del C:\mvxout a C:\mvxout\services\common.
- Cambiar el Temp Directory de C:\mvxout a C:\mvxout\services\common, marcar el strs.lic y escoger Open.
- Cambiar Argument File de C:\mvxout a C:\mvxout\services\streamserve1.arg

Contactos

- Nombre:
- Cargo:
- Teléfono:

Procedimiento de Recuperación de Central Telefónica

Objetivo

Establecer el procedimiento en una situación de contigencia por falla central telefónica

Equipos involucrados

Central Telefónica Quito – Carapungo

Recuperación

Comunicarse con Proveedor
Contactos de Soporte

Nombre	Responsabilidad	Contacto	TE Oficina	TE Celular
Intelcom	Soporte Central telefónica	Milton Rosero	593 2 2-955-292	593 9 4753339

Contactos

- Nombre:
- Cargo:
- Teléfono:

Procedimiento de Recuperación de estaciones de trabajo

Objetivo

Esta documentación tiene como objetivo tener un proceso para la realización de imágenes en las maquinas nuevas que trabajaran en cualquier de las estaciones de Ecuador: comprendiendo Quito, Guayaquil, Carapungo. La utilización de este documento será única y exclusivamente por personal de IT y personas autorizados para cualquier proceso de auditoría o similar a este.

Proceso

Antes de realizar la Imagen debemos de tener en cuenta que esta aplicación será cargada únicamente en maquinas estándares que Israriego sugiere:

HP DC5800
HP 6910p – hp 6930P
Cargar el CD de booteo BUILD en la unidad que se desea cargar la imagen.
Elegir la opción 1 para continuar con el proceso.
XXXX es el nombre del servidor en donde están las configuraciones para realizar la imagen.
Seguir los pasos que nos especifica la pagina.
Reiniciar equipo

Comenzara a cargar automáticamente el Windows XP Profesional.

Luego aparecerán opciones para configurar el idioma, lugar y hora e información del país:

Build Location: Israriego-ECUADOR
Build Types: NEW DEPLOYMENT
EDC Record: EDC not use
EDC Record Comment: Deploy in Quito

Posteriormente cargará los siguientes programas adicionales:

Microsoft Office 2007
Microsoft Communicator 2007
PgP Desktop (Únicamente en Laptop)
Cyber Armor (Únicamente en Laptop)
Israriego VpN (Únicamente en Laptop)
NetMeeting
Webex
SAP
Win Zip
Oracle
Symantec Client Security

Especificación de imágenes

Técnicamente se instalaran las aplicaciones antes mencionadas, además también de los drivers de sonido, pantalla, wireless, dispositivos usb, etc.

Verificación de Imágenes

Al finalizar el proceso de imágenes de BUILD se realiza las pruebas respectivas como el acceso los programas, acceso a la red e internet, acceso al correo electrónico, VPN si fuera el caso de una laptop, Communicator.

Contactos

Nombre:
Cargo:
Teléfono:

Proceso de Compra de equipos

Objetivo

Esta documentación tiene como objetivo tener un proceso para la compra de equipos específicos que requiere Israriego, hardware con especificaciones técnicas especiales, con padrones que exige la empresa, las mismas que serán administradas en cada uno de los sitios de la Unidad.

La utilización de este documento será única y exclusivamente por personal de IT y personas autorizados para cualquier proceso de auditoría o similar a esto.

A través de esta documentación se podrá conocer los nombres de los Proveedores, modelos de equipos, y el proceso exacto de compra.

Compra

Proceso de Compra de Laptops y Work Station HP

Antes de realizar la compra se hace un estudio de las necesidades del usuario que trabajara con la maquina a ser comprada, decidida su necesidad y maquina procedemos a pedir 2 cotizaciones a nuestros principales proveedores de HP en Ecuador:

Compsesa
Binaria Sistemas

Los modelos plantillas de Israriego para adquirir son:

HP DC5800 (Work Station)
HP 6910p (Laptop)
Carepack (5 años para Wok Stations)
Carepack (4 años para Laptop)

Se pide vía email una cotización de los modelos especificados a los 2 proveedores y se escoge el mejor precio, considerando que nosotros tenemos un contrato Atlas el mismo que tenemos descuentos y formas de entrega más rápido.

Proceso de Compra de Servidores HP

Este proceso es exactamente igual al de las maquinas y laptops ya que estos mismo proveedores son aquellos que trabajan con servidores HP, así como también con el contrato atlas que tenemos con ellos.

Los servidores plantillas que compramos son:

HP DL380G5 Mod-FX
Carepack (5 años para servidores)

Se elige entre los 2 proveedores el mejor precio, y se realiza la compra.

Únicamente los modelos de HP especificados, son aquellos que entran en el contrato Atlas de HP.

Proceso de Compra de Routers y Wireless CISCO

Otros

Generalmente el script esta diseñado para realizar backup's de todos los datos en forma obligatoria e inclusive cuando haya error de conexión, pero no permite hacer copias cuando estén estos datos en uso, es decir si algún usuario esta haciendo uso de este archivo, el script lo que hace es saltar este archivo para continuar con el siguiente, pero es corregido al momento de hacer nuevamente el Backup.

Existen discos externos de 1 Tera en cada localización en donde se hacen respaldos solo de los datos del servidor local, se hicieron pruebas para hacer un Backup consolidado de los 3 servidores pero por problemas de red y demasiada información no hubo esta posibilidad.

Contactos

Nombre:
Cargo:
Teléfono:

En este espacio se deben adjuntar todos los acuerdos y contratos con proveedores, por motivos de privacidad y confidencialidad no es posible publicarlos.

Mantenimiento y Prueba del Plan

Esta sección contiene el cronograma de tareas a realizar anualmente para el mantenimiento y prueba de este Plan DRP.

Tareas de Mantenimiento

Ítem	Maintenance Plan Item	Responsibility	Schedule
1	Mantenimiento del Folder DRP de la unidad Plastro Argentina en un Server local.	DRP Coordinator	Continuo
2	Actualizar la lista de contactos de proveedores, personal, emergencia, etc.	DRP Coordinator	Trimestral
3	Revisión completa del Plan DRP identificando los cambios en los ARTO, IRTO, RPO y Prioridad de Recuperación, etc. Luego de la revisión, realizar las siguientes actividades: -Obtener las aprobaciones requeridas, -Generar las copias físicas y digitales, e impresiones necesarias, reemplazando las versiones anteriores.	DRP Coordinator	Anual
4	Preparar, actualizar y conducir el Plan de Pruebas del presente Plan, el cual se encuentra en el documento adjunto.	DRP Coordinator	Anual
5	Enviar el presente documento actualizado al BCP Coordinator para su inclusión en el BCP Plan de la Unidad.	DRP Coordinator	Cada vez que cambie

Ejemplo Plan de pruebas

ID	Tarea	Descripción	Coordinador	Fecha	Observaciones

Change Log

Description of change	Name	Date	Version

ANEXO 12

REGISTRO DE NOTIFICACIÓN A CONTACTOS

Registro de notificaciones a contactos					
Empleado llamado por	**Fecha**	**Nombre de persona llamada**	**Hora de llamada**	**Resultado de llamada**	**Comentarios**

ANEXO 13

ANÁLISIS DE IMPACTO AL NEGOCIO - BIA

-Preguntas a Liderazgo- **-Preguntas Gerente de Procesos**

-Completar un formulario para cada proceso crítico

Cuál es el proceso crítico?: Contratación de personas clave – RRHH

RTO: Cual es el tiempo mínimo aceptable o permitido que este proceso puede ser interrumpido, antes que la interrupción provoque un impacto significativo en la organización? **15**

Resaltar una: Horas **Día(s)** Semana(s) Mes(es)

El período de tiempo indicado anteriormente se conoce desde este momento como Tiempo Objetivo de Recuperación. (RTO).

Cuál es el Objetivo de punto de recuperación (RPO)? **15 días** (esto refleja la frecuencia en que los datos de este proceso son respaldados / cantidad máxima de datos de la empresa que puede permitirse el lujo de perder)

Una interrupción que exceda el RTO *puede* causar impacto significativo a:

Pérdida de venta o ingresos: ☒ SI ☐ NO

Describir: Pérdida de Ventas relacionadas con la falta de personal clave de ventas.

Satisfacción del cliente externo ☒ SI ☐ NO

Describir: Pérdad de personal de ventas o atención al cliente, personal clave.

Cliente Interno o Proceso organizacional ◉ SI ○ NO

Describir: Pérdida de personal que conozca los procesos claves de la compañía.

Relaciones comerciales con Proveedor ○ SI ◉ NO

Describir:

Cumplimiento de obligaciones legales: ○ SI ◉ NO

Describir:

Otros:

Describir:

Este proceso requiere conectividad a la red? ◉ SI ○ NO

Este proceso requiere conexión a internet? ◉ SI ○ NO

Análisis de impacto al negocio BIA

-Preguntas a Liderazgo- **-Preguntas Gerente de Procesos**

-Completar un formulario para cada proceso crítico

Cuál es el proceso crítico?: Producción y Cadena de suministros

RTO: Cual es el tiempo mínimo aceptable o permitido que este proceso puede ser interrumpido, antes que la interrupción provoque un impacto significativo en la organización? **8**

Resaltar una: Horas **Día(s)** Semana(s) Mes(es)

El período de tiempo indicado anteriormente se conoce desde este momento como Tiempo Objetivo de Recuperación. (RTO).

Cuál es el Objetivo de punto de recuperación (RPO)? **1 día** (esto refleja la frecuencia en que los datos de este proceso son respaldados / cantidad máxima de datos de la empresa que puede permitirse el lujo de perder)

Una interrupción que exceda el RTO *puede* causar impacto significativo a:

Pérdida de venta o ingresos: ☒ SI ☐ NO

Describir: Pérdida de Ventas. Una vez que el inventario se agota no es posible proveer al cliente.

Satisfacción del cliente externo ☒ SI ☐ NO

Describir: La Compañía no puede entregar productos en la fecha de acordadas con el cliente

Cliente Interno o Proceso organizacional ☒ SI ☐ NO

Describir: Ventas, proceso de Instalación proyectos, clientes internos no podrían realizar la solicitud de material para instalaciones.

Relaciones comerciales con Proveedor ☐ SI ☒ NO

Describir:

Cumplimiento de obligaciones legales: ☐ SI ☒ NO

Describir:

Otros:

Describir:

Este proceso requiere conectividad a la red? ☒ SI ☐ NO

Este proceso requiere conexión a internet? ☒ SI ☐ NO

Análisis de impacto al negocio BIA

-Preguntas a Liderazgo- **-Preguntas Gerente de Procesos**

-Completar un formulario para cada proceso crítico

Cuál es el proceso crítico?: Proceso Control Finanzas

RTO: Cual es el tiempo mínimo aceptable o permitido que este proceso puede ser interrumpido, antes que la interrupción provoque un impacto significativo en la organización? **3**

Resaltar una: Horas **Día(s)** Semana(s) Mes(es)

El período de tiempo indicado anteriormente se conoce desde este momento como Tiempo Objetivo de Recuperación. (RTO).

Cuál es el Objetivo de punto de recuperación (RPO)? **1 día** (esto refleja la frecuencia en que los datos de este proceso son respaldados / cantidad máxima de datos de la empresa que puede permitirse el lujo de perder)

Una interrupción que exceda el RTO *puede* causar impacto significativo a:

Pérdida de venta o ingresos: ☒ SI ☐ NO

Describir: Es posible la pérdida de ingresos por ventas, debido a la falta de colección de cobros y debido a esto la falta de control en el despacho de productos.

Satisfacción del cliente externo ☒ SI ☐ NO

Describir: Control del proceso de facturación debido a la demora en el proceso de autorizaciones de facturación y despacho por créditos.

Cliente Interno o Proceso organizacional ☒ SI ☐ NO

Describir: Puede haber retrasos debido a la que esto causaría pérdida de recursos de pago de roles, gerente de operaciones y cadena de suministros. Esto puede causar pérdida de control en los ingresos por tesorería.

Relaciones comerciales con Proveedor ☒ SI ☐ NO

Describir: Demora en pago a proveedores y emisión de retenciones.

Cumplimiento de obligaciones legales: ☒ SI ☐ NO

Describir: Demora en el pago de impuestos, declaración de balances, posible demanda de proveedores, y dificultades en recolección de datos.

Otros:

Describir:

Este proceso requiere conectividad a la red?

☒ SI ☐ NO

Este proceso requiere conexión a internet?

☒ SI ☐ No

ANEXO 14

PLAN DE RECUPERACIÓN

Por favor complete esta planilla para cada proceso crítico, proceso durante operaciones normales

Nombre del proceso crítico: ***Producción y cadena de suministros***

Nombre del Gerente del Proceso: Luis Millán

Note: *El gerente del proceso es responsable de desarrollar y activar el plan de recuperación para este proceso crítico, definir prioridades, buscar soluciones y conducir el mantenimiento anual del plan en cooperación del coordinador del BCP.*

Cual es el tiempo objetivo de recuperación: (RTO)? 8 días

Nota: *El tiempo objetivo de recuperación es el tiempo máximo aceptable fuera de operación para este proceso crítico; este proceso debió ser identificado en el BIA.*

PERSONAL (EMPLEADOS, TERCEROS)

Que eventos podrían conducir a una pérdida de personal en este proceso: llenar en orden de probabilidad

Erupción Volcánca

Terremoto

Pandemia

Fuego

Desorden civil

Existen personas de respaldo para los puestos críticos de este proceso?

☐ Si ☉ No, Explique porqué:

Por favor explique las acciones que usted tomaría para mitigar o prevenir un evento que provoque una potencial pérdida de personal clave que soporta este proceso o porque no son necesarias tomar medidas de precaución:

- Cumplimiento de políticas de fábrica
- Familiarización con el plan de emergencia
- Puestos de respaldo en otras áreas de la empresa.

Cuál es el plan (papel) para los empleados que no son críticos y que soportan este proceso durante un evento de corte de actividades? ¿Van a trabajar desde casa? Trabajará desde casa (con sueldo o sin sueldo?)

XXXXXXX

Información adicional:

TECNOLOGÍA DE LA INFORMACIÓN (I.T.)

Qué eventos pueden llevar a una pérdida de Tecnologías de la Información que apoya este proceso crítico? (En orden de probabilidad)

Corte de energía

Corte de red LAN

Amenaza de incendio

Erupción volcánica

Terremoto

Liste el software/aplicaciones que soportan este proceso crítico durante las operaciones normales (que pueden ser alojados en servidores locales)

Nombre de Software/Aplicación-Alojamiento Local?-Si es local, cual es el RPO*?

Movex	Israel	1 días
Software de PLC	Local	1 días
WCADI	Local	5 días
LM tools	Local	5 días

*RPO = Recovery Point Objective

Para operaciones normales, que hardware es requerido para que este proceso funcione?

No. Desktops: 16

No. Laptops: 3

Cómo deben ser configurados estos equipos? (Software especial, programas, etc.)

Número de máquinas servidores: 2

Tipo de red: VPN

Routers: 1

Switches: 10

Número de impresoras: 7 Tipo de impresoras?: 6 Laser - 1 matricial

Número de copiadoras: 2 Blanco y negro

Número de fax: 3

Número de teléfonos: 15

Otros: Teléfono móvil – 1 Adicional

INSTALACIONES

Qué eventos pueden conducir a una pérdida temporal de la instalación o lugar de trabajo (o el acceso a las instalaciones), que apoya este proceso crítico? (En orden de probabilidad)

Corte de energía

Terremoto

Amenaza de fuego

Erupción volcánica

Paro, huelga.

Existe una unidad alternativa de trabajo?

 Si, agregue información. Unidad Chile, Unidad Argentina, Unidad Brasil

☐ No, explique:

Se han hecho arreglos para llevar a cabo este proceso crítico en una ubicación alternativa? ¿Tiene un contrato pendiente de pago?

☒ Si, agregue información. No hay contratos adquiridos – unidad Chile, unidad Argentina, unidad Brasil

☐ No, explique:

Si "No", puede otra unidad desempeñar este proceso crítico?

☒ Si, que unidades?: Unidad Chile, Unidad Argentina, unidad Brazil

☐ No, siga con la siguiente pregunta

Tiene una lista de otros equipos críticos que crea necesarios y una lista de proveedores que puedan proveerlo para completar este proceso crítico?

☐ Yes ☒ No

Información adicional:

Si usted respondió "No", entonces desarrolle el siguiente checklist para este proceso crítico?

Función de procesos		
☐	Mis necesidades de espacio de trabajo actuales son.	
☐	Necesito un número ___ de metros cuadrados para llevar a cabo mis operaciones	
☐	Necesito ubicar a _____ personas en el edificio.	
☐	Necesito ___ metros cuadrados de espacio para almacenamiento.	
☐	Necesito el siguiente tipo de características para el espacio de trabajo.	
☐	El área de trabajo debe tener el siguiente tipo de piso	
Incendio, vida y seguridad		
☐	Debido a la naturaleza del trabajo realizado durante los procesos de nuestro trabajo, tenemos que tener en consideración a los siguientes riesgos que se generan. (por ejemplo, la necesidad de una extinguidores de la clase D, nuestra operaciones de rociado de VOC pesada y requiere ventilación especial, etc...)	
Seguridad		
☐	Debido a la naturaleza de nuestro trabajo necesitamos las siguientes características de seguridad: (por ejemplo puerto de seguridad, área de trabajo, etc=	
Telecomunicaciones		
☐	Necesitamos los siguientes requerimientos en telecomunicaciones para ejecutar nuestras operaciones.	
Aire acondicionado		
☐	El espacio debe proveer aire acondicionado	
☐	Las operaciones requieren cierto nivel de humedad	
Electricidad		
☐	Los procesos requieres un generador de electricidad alterno en la propiedad	
☐	Nuestros requerimientos específicos de energía son:	
☐	Necesitamos el siguiente tipo de energía disponible. (110V, 208V, 480V)	
Cableado – infraestructura		
☐	Nuestras operaciones necesitan la siguiente infraestructura de voz y datos	
Despachos		
☐	Necesitamos un lugar de carga disponible	
Cuarto de servidores		
☐	Necesitamos un cuarto de servidores en un espacio disponible, explicar si necesita aire acondicionado, tipo de piso, tipo de pared, voltaje, etc.	
☐	Es necesario un sistema de distribución de energía eléctrica?	
☐	Es necesario un sistema de UPS en la sala?	

Información adicional:

Siguientes pasos…

Tras la finalización de esta plantilla, debe ser completado el plan de reanudación.

Un plan de reanudación (procedimiento de solución) debe requerir menos recursos para ejecutar que los necesarios para las operaciones normales. Haga una lista de los recursos mínimos necesarios para su reanudación.

Crear una estrategia de recuperación para cada uno de estos recursos. Los recursos necesarios para la reanudación deben ser recuperados en primer lugar. Identificar las acciones que se pueden tomar para proteger estos recursos mínimos a partir de las amenazas conocidas - reducir riesgos.

PLAN DE RECUPERACIÓN

Por favor complete esta planilla para cada proceso crítico, proceso durante operaciones normales

Nombre del proceso crítico: ***Control de fondos***

Nombre del Gerente del Proceso: Deneff Carranza

Note: *El gerente del proceso es responsable de desarrollar y activar el plan de recuperación para este proceso crítico, definir prioridades, buscar soluciones y conducir el mantenimiento anual del plan en cooperación del coordinador del BCP.*

Cual es el tiempo objetivo de recuperación: (RTO)? 3 días

Nota: El tiempo objetivo de recuperación es el tiempo máximo aceptable fuera de operación para este proceso crítico; este proceso debió ser identificado en el BIA.

PERSONAL (EMPLEADOS, TERCEROS)

Que eventos podrían conducir a una pérdida de personal en este proceso: llenar en orden de probabilidad

Erupción Volcánica

Terremoto

Pandemia

Fuego

Desorden civil

Existen personas de respaldo para los puestos críticos de este proceso?

☐ Si

☉ No, Explique porqué: La habilidad y responsabilidad para aprobar transacciones solo las realiza el controller

Por favor explique las acciones que usted tomaría para mitigar o prevenir un evento que provoque una potencial pérdida de personal clave que soporta este proceso o porque no son necesarias tomar medidas de precaución:

- Cumplimiento de políticas de fábrica
- Familiarización con el plan de emergencia
- Puestos de respaldo en otras áreas de la empresa.

Cuál es el plan (papel) para los empleados que no son críticos y que soportan este proceso durante un evento de corte de actividades? ¿Van a trabajar desde casa? Trabajará desde casa (con sueldo o sin sueldo?)
Información adicional:

TECNOLOGÍA DE LA INFORMACIÓN (I.T.)

Qué eventos pueden llevar a una pérdida de Tecnologías de la Información que apoya este proceso crítico? (En orden de probabilidad)

Corte de energía

Corte de red LAN

Amenaza de incendio

Erupción volcánica

Terremoto

Liste el software/aplicaciones que soportan este proceso crítico durante las operaciones normales (que pueden ser alojados en servidores locales)

Nombre de Software/Aplicación-Alojamiento Local?-Si es local, cual es el RPO*?

Movex	Israel	1 días
Microsoft office SQL	Local	3 días
Cash managment	Local	3 días
E-mail	Local	3 días

*RPO = Recovery Point Objective

Para operaciones normales, que hardware es requerido para que este proceso funcione?

No. Desktops: 8

No. Laptops: 8

Cómo deben ser configurados estos equipos? (Software especial, programas, etc.)

Número de máquinas servidores: 1

Tipo de red: VPN

Routers: 1

Switches: 4

Número de impresoras: 5 Tipo de impresoras?: 4 Láser - 1 matricial

Número de copiadoras: 1 Blanco y negro

Número de fax: 2

Número de teléfonos: 17

Otros: Teléfono móvil – 3 Adicional

INSTALACIONES

Qué eventos pueden conducir a una pérdida temporal de la instalación o lugar de trabajo (o el acceso a las instalaciones), que apoya este proceso crítico? (En orden de probabilidad)

- Corte de energía local
- Corte de energía regional
- Corte de red LAN
- Ataque cibernético

Existe una unidad alternativa de trabajo?

☉ Si, agregue información. Unidad de Carapungo

☐ No, explique:

¿Se han hecho arreglos para llevar a cabo este proceso crítico en una ubicación alternativa? ¿Tiene un contrato pendiente de pago?

☒ Si, agregue información. No hay contratos adquiridos – unidad Carapungo

☐ No, explique:

Si "No", puede otra unidad desempeñar este proceso crítico?

☐ Si, ¿que unidades?:

☒ No, siga con la siguiente pregunta

¿Tiene una lista de otros equipos críticos que crea necesarios y una lista de proveedores que puedan proveerlo para completar este proceso crítico?

☐ Yes

☒ No

Información adicional:

Si usted respondió "No", entonces desarrolle el siguiente checklist para este proceso crítico

Función de procesos		
☐	Mis necesidades de espacio de trabajo actuales son.	
☐	Necesito un número ___ de metros cuadrados para llevar a cabo mis operaciones	
☐	Necesito ubicar a _____ personas en el edificio.	
☐	Necesito ___ metros cuadrados de espacio para almacenamiento.	
☐	Necesito el siguiente tipo de características para el espacio de trabajo.	
☐	El área de trabajo debe tener el siguiente tipo de piso	
Incendio, vida y seguridad		
☐	Debido a la naturaleza del trabajo realizado durante los procesos de nuestro trabajo, tenemos que tener en consideración a los siguientes riesgos que se generan. (por ejemplo, la necesidad de una extinguidores de la clase D, nuestra operaciones de rociado de VOC pesada y requiere ventilación especial, etc...)	
Seguridad		
☐	Debido a la naturaleza de nuestro trabajo necesitamos las siguientes características de seguridad: (por ejemplo puerto de seguridad, área de trabajo, etc=	
Telecomunicaciones		
☐	Necesitamos los siguientes requerimientos en telecomunicaciones para ejecutar nuestras operaciones.	
Aire acondicionado		
☐	El espacio debe proveer aire acondicionado	
☐	Las operaciones requieren cierto nivel de humedad	
Electricidad		
☐	Los procesos requieres un generador de electricidad alterno en la propiedad	
☐	Nuestros requerimientos específicos de energía son:	
☐	Necesitamos el siguiente tipo de energía disponible. (110V, 208V, 480V)	
Cableado – infraestructura		
☐	Nuestras operaciones necesitan la siguiente infraestructura de voz y datos	
Despachos		
☐	Necesitamos un lugar de carga disponible	
Cuarto de servidores		
☐	Necesitamos un cuarto de servidores en un espacio disponible, explicar si necesita aire acondicionado, tipo de piso, tipo de pared, voltaje, etc.	
☐	Es necesario un sistema de distribución de energía eléctrica?	
☐	Es necesario un sistema de UPS en la sala?	

Información adicional:

Siguientes pasos…

Tras la finalización de esta plantilla, debe ser completado el plan de reanudación.

Un plan de reanudación (procedimiento de solución) debe requerir menos recursos para ejecutar que los necesarios para las operaciones normales. Haga una lista de los recursos mínimos necesarios para su reanudación.

Crear una estrategia de recuperación para cada uno de estos recursos. Los recursos necesarios para la reanudación deben ser recuperado en primer lugar. Identificar las acciones que se pueden tomar para proteger estos recursos mínimos a partir de las amenazas conocidas - reducir riesgos**.**