



Universidad Técnica Particular de Loja
La Universidad Católica de Loja

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

TEMA:

PLAN DE CONTINUIDAD DE NEGOCIOS EN EL ÁMBITO EDUCATIVO

Tesis previa a la obtención del Título de Ingeniero en Informática

Autor:

Fabián Patricio Martínez Bermúdez

Directoras:

Ing. Mayra Romero L.

Ing. Silvana Jiménez R.

Loja – Ecuador

2010

CERTIFICACIÓN

Ing. Mayra Romero L.

DIRECTOR DE TESIS

Ing. Silvana Jiménez

CODIRECTOR DE TESIS

CERTIFICA:

Que el presente trabajo de tesis realizado por Fabián Patricio Martínez Bermúdez cuyo tema es Plan de Continuidad de Negocios en el ámbito educativo, ha sido dirigido, orientado y evaluado en todas sus fases, habiendo constatado que cumple con los requisitos de fondo y forma exigidos por la Escuela de Ciencias de la Computación, en consecuencia autorizo su presentación, sustentación y defensa.

Ing. Mayra D. Romero L

DIRECTORA

Ing. Silvana Jiménez R.

CODIRECTORA

Loja, marzo de 2010

CESIÓN DE DERECHOS

Yo, Fabián Patricio Martínez Bermúdez, declaro ser autor del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través o con el apoyo financiero, académico o institucional (operativo) de la Universidad.

.....

Fabián Patricio Martínez Bermúdez

AUTORÍA

Los conceptos, ideas opiniones desarrolladas en el presente trabajo son de exclusiva responsabilidad del autor.

.....

Fabián Patricio Martínez Bermúdez

AGRADECIMIENTO

En la vida, encontrar las oportunidades para poder triunfar en ocasiones se tornan inciertas y muchas de ellas imposibles cuando no se tiene el coraje y la decisión de querer hacerlo, sin embargo, en mi caso esa decisión se la agradezco en primer lugar a Dios, como eje fundamental de mi vida, pero sobretodo a mi madre, quién ha sido el único ser humano que no perdió nunca la fe en mí, y que con sus continuas oraciones, su sonrisa gentil, su voz firme en ocasiones permitió que el presente proyecto haya llegado a su feliz término. Dios te pague mamacita. Tu eres quién me dio el coraje y solventó mi decisión.

DEDICATORIA

A mis hijas, Gabby, Dianny y Patty, quienes constituyen la razón de encontrarle sentido a todo esfuerzo que me permite crecer como persona, profesional y sobretodo como ser humano.

A ti, Lore, quien me permitió encontrarle matiz a mi vida y has sido un aporte valioso para la construcción de mi tesis, tu continuo y desinteresado apoyo logró construir palabra a palabra este PCN que gracias a ti llegó a feliz término. Gracias de todo corazón y recuerda siempre que yo a ti te quiero mucho.

ESQUEMA DE CONTENIDOS

Contenido

INTRODUCCIÓN	11
1. Fase Preliminar del Plan de Continuidad de Negocios (PCN)	13
1.1. Beneficios de Desarrollar un Plan de Continuidad de Negocios	13
1.2. Aprobación y comunicación del contenido del PCN	14
1.3. Definición de políticas en la planeación del Plan de Continuidad de Negocios (PCN).	15
1.4. Presupuesto preliminar para el desarrollo del PCN	16
1.5. Organización del equipo del proyecto	21
2. Identificación de los Servicios Críticos de la Institución	23
2.1. Servicio Académico	24
2.2. Servicio Gestión Humana	27
2.3. Servicio de Admisión	30
2.4. Servicio de Mantenimiento y Reparaciones.	33
2.5. Servicio de Auditoría	35
2.6. Servicio de Colecturía	37
3. Priorización de los Servicios Críticos	39
4. Desarrollo e Implementación del PCN.	44
4.1. RIESGOS GENERALES	45
4.2. RIESGOS POR SERVICIO	46
4.2.1. Riesgos del Servicio de Admisión.	46
4.2.1.1. Consecuencias del Servicio	47
4.2.2. Riesgos del Servicio de Colecturía.	47
4.2.2.1. Consecuencias del Servicio	48
4.2.3. Riesgos del Servicio de Mantenimiento y Reparaciones.	48
4.2.3.1. Consecuencias del Servicio	49
4.2.4. Riesgos del Servicio Académico.	49
4.2.4.1. Consecuencias del Servicio	50
4.2.5. Riesgos del Servicio de Gestión Humana.	50
4.2.5.1. Consecuencias del Servicio	51

4.2.6.	Riesgos del Servicio de Auditoría.	52
4.2.6.1.	Consecuencias del Servicio	52
5.	Seguridades a los Servicios Críticos.	53
5.1.	Seguridades Generales a los Servicios Críticos	53
5.2.	Seguridades por Servicio	54
5.2.1.	Servicio de Admisión	54
5.2.2.	Servicio de Colecturía	54
5.2.3.	Servicio de Mantenimiento y Reparaciones	55
5.2.4.	Servicio Académico	56
5.2.5.	Servicio de Gestión Humana	56
5.2.6.	Servicio de Auditoría	57
6.	Sistema de Comunicaciones	59
6.1.	Especificaciones, sistemas de comunicación y dependencias de la Institución	59
6.2.	Personal Clave	60
6.3.	Servicios externos de emergencia	61
7.	Planes del PCN	62
7.1.	Plan de Recuperación del Negocio	62
7.1.1.	Autoridades en el mantenimiento del edificio	62
7.1.1.1.	Instalaciones Propias.	62
7.2.	Fase de Recuperación del Negocio	71
7.2.1.	Movilización del Equipo de Recuperación del Negocio	71
7.2.2.	Evaluación del daño e impacto en la Institución	72
7.2.3.	Plan específico de recuperación	73
7.2.4.	Monitoreo del Servicio	74
7.2.5.	Mantener a todos informados	74
7.2.6.	Reporte de la fase de recuperación del negocio	75
7.3.	Actividades de Recuperación del Negocio	75
7.3.1.	Suministro eléctrico	75
7.3.2.	Sistema de Comunicaciones	76
7.3.3.	Sistemas de la Tecnología de la Información	76
7.3.4.	Recursos Humanos	76
7.3.5.	Información y documentación	76
7.3.6.	Operaciones y administración	77
8.	PROTECCION	83
8.1.	Organigrama funcional	83
8.2.	Estrategias de backups y recuperación de los sistemas IT	84
8.3.	Cobertura de Seguro	86

8.4.	Proveedores y personal clave del PCN	87
8.4.1.	Equipo de Recuperación del Desastre	87
8.4.2.	Equipo de Recuperación del Negocio	88
8.5.	Procedimientos y documentación clave	88
8.5.1.	Documentos y registros vitales de procesos de la Institución	88
8.5.2.	Almacenamiento fuera de la Institución	88
8.5.3.	Procedimientos para el manejo de padres de familia, proveedores y público en general	89
8.5.4.	Autorización para la protección en caso de emergencia	89
9.	CAPACITACIÓN DEL PERSONAL	90
9.1.	Gestión del Proceso	90
9.1.1.	Objetivos y Alcance	90
9.1.2.	Necesidades de la Capacitación	91
9.1.3.	Material de capacitación	91
9.1.4.	Agenda preliminar de capacitación	91
9.1.5.	Comunicación	92
9.2.	Evaluación de la Capacitación	93
9.2.1.	Cuestionarios	93
9.2.2.	Evaluación de la retro alimentación	95
10.	PRUEBAS DE VALIDACIÓN	96
10.1.	Planificación de las pruebas	96
10.1.1.	Objetivos y alcance de las pruebas	96
10.1.2.	Ambiente de las pruebas	96
10.1.3.	Conducción de las pruebas	106
10.1.4.	Retroalimentación	106
10.1.5.	Presupuesto para la fase de prueba	106
10.1.6.	Capacitación	107
10.2.	Conducción de las pruebas	107
10.2.1.	Evaluación de los resultados de las pruebas	108
11.	MANTENIMIENTO	109
11.1.	Control de cambio	109
11.2.	Responsabilidades de mantenimiento	110
11.3.	Pruebas de mantenimiento	111
11.4.	Responsable de capacitación	111
12.	CONCLUSIONES	112
13.	RECOMENDACIONES	113
14.	ANEXOS	114
14.1.	ANEXO 1	114

14.1.1.	NORMA ISO 27002:2005	114
14.2.	ANEXO 2	116
14.2.1.	NORMA ISO 9001 – 2008	116
14.3.	ANEXO 3	123
14.3.1.	Entrevista a los Administradores de los Servicios Críticos	123
	Servicio de Admisión	124
	Servicio de Colecturía	129
	Servicio de Mantenimiento y Reparaciones	132
	Servicio Académico	135
	Servicio Gestión Humana	138
	Servicio Auditoría	141
14.4.	ANEXO 4	144
14.4.1.	Hardware del Servicio de Admisión	144
14.4.2.	Software del Servicio de Admisión	144
14.4.3.	Hardware del Servicio de Mantenimiento y Reparaciones (Laboratorio de Computación)	144
14.4.4.	Software del Servicio de Mantenimiento y Reparaciones (Laboratorio de Computación)	145
14.4.5.	Hardware del Servicio de Mantenimiento y Reparaciones (Laboratorio de Contabilidad)	146
14.4.6.	Software del Servicio de Auditoría (Laboratorio de Contabilidad)	147
14.4.7.	Aplicaciones del Servicio de Auditoría (Laboratorio de Contabilidad)	147
14.5.	ANEXO 5	149
14.5.1.	COBERTURA DE DOCENTES Y ESTUDIANTES	149
14.6.	ANEXO 6	151
14.6.1.	BOTIQUIN DE PRIMEROS AUXILIOS	151
Glosario		152
Bibliografía		153

INTRODUCCIÓN

En toda empresa se necesita garantizar la eficiencia y permanencia en los servicios, el proyecto está orientado a establecer planes de aseguramiento en continuidad de procesos, en la primera fase se realizará un levantamiento de datos donde se podrá tener una visión sobre la preparación del establecimiento educativo en el caso de desastres, o emergencias, y se definirán políticas para la elaboración de un Plan de Continuidad de Negocios

En la segunda fase, desarrollaremos un conjunto de entrevistas para la identificación de los servicios que maneja la Institución, con la finalidad de conocer cuáles son los principales activos, para lo que se definen seis servicios: Académico, Admisión, Auditoría, Colecturía, Gestión Humana, Mantenimiento y Reparaciones.

En la tercera fase, definiremos los servicios de mayor relevancia basados en los resultados obtenidos en la segunda fase, para con ello poder determinar aquellos servicios considerados más críticos.

En la cuarta fase, desarrollaremos e implementaremos el PCN para analizar los riesgos generales del colegio, y en idéntica forma los riesgos particulares por Servicio, definiendo junto a ello las causas que generan el riesgo, determinando su probabilidad e impacto y definiendo cuáles son los bienes que se encuentran en riesgo.

En la quinta fase, una vez definidos los parámetros expuestos en el párrafo previo, estableceremos las seguridades para afrontar dichos riesgos, identificando la consecuencia y procurando la solución más viable.

En la sexta fase, orientaremos el PCN para determinar cuáles son las especificaciones, sistemas de comunicación y dependencias de la Institución, con el objeto de definir el personal clave y los servicios de emergencia.

En la séptima fase, estableceremos los planes de recuperación de negocio, y en su conjunto las fases y actividades para la recuperación descrita, con el objeto de definir como se movilizarán los equipos de recuperación del negocio, como se evaluarán los daños y que planes serán creados para lograr recuperar a la Obra Educativa en el menor tiempo posible.

En la octava fase, analizaremos los modos adecuados de garantizar la mejor protección al establecimiento, definiendo políticas de respaldo, una cobertura de seguro y los procedimientos y documentación clave.

En la novena fase, es lógico considerar, que si queremos que el PCN actúe en modo adecuado, será imprescindible que quienes forman parte del mismo sean capacitados, por lo que es necesario realizar la planificación de las capacitaciones y la conducción de estas.

En la décima fase, se realizarán pruebas de validación a través de simulacros, con el objeto de verificar si se cumple con el objetivo y alcance, si el ambiente es adecuado y si la conducción va encaminada acorde a lo establecido en el PCN, para comprobar realizaremos la retroalimentación respectiva.

En la undécima fase, una vez los miembros capacitados, se deberá dar un mantenimiento continuo al PCN, por ello se recogerá información que permita conocer las responsabilidades del mantenimiento, el control del cambio y las pruebas requeridas del mismo.

Para terminar, enfocaremos el tema del PCN no solo como una manera de mantenerse a flote sino como una estrategia que mantendrá la buena reputación de la Obra Educativa “Nuestra Señora del Rosario”.

Así mismo, queremos realzar el hecho de que la Institución se está acogiendo a la Norma ISO 9001 – 2008, es por ello que consideramos básico generar reportes, para que los equipos de auditoría tomen en cuenta estos temas para el buen funcionamiento de las salas. A esto se añaden, en el desarrollo de la presente tesis, los criterios de tecnología de la información que constan en el COBIT y que son parte de la Norma ISO 27002:2005, como un modo de contribución para alcanzar el objetivo propuesto por la Obra Educativa.

1. Fase Preliminar del Plan de Continuidad de Negocios (PCN)

1.1. Beneficios de Desarrollar un Plan de Continuidad de Negocios

Iniciando en un contexto generalizado, en nuestro país particularmente, el Desarrollo de un Plan de Continuidad de Negocios es algo desconocido, por ende, el saber aprovechar de sus beneficios se torna algo utópico, en mayor medida aún, para las instituciones de carácter educativo quienes carecen en forma mayoritaria de una idea clara de este nuevo concepto.

Es por eso que consideramos pertinente que se debe, a quienes han decidido aplicarlo, darles una idea clara hacia donde se orienta el Plan de Continuidad de Negocios (PCN) como se describirá en el desarrollo de la tesis. En el ámbito educativo sería útil dejar claro que las instituciones que dediquen tiempo y recursos al planeamiento de la continuidad del negocio, han de saber de la importancia de estos planes para proteger la seguridad de sus estudiantes, los departamentos y del personal. Han de reconocer la importancia de la planeación de continuidad del negocio, y contar con los individuos con los conocimientos y entrenamiento en caso de un desastre. Han de tomar en cuenta que la continuidad del negocio debe ser un factor para el establecimiento, identificación y control de riesgos, políticas, guías prácticas y procedimientos rutinarios, y que todo el personal en la institución debe saber qué hacer cuando un desastre ocurra.

“El principal objetivo de un plan de continuidad del negocio es proporcionar mecanismos que provean a una entidad la capacidad de reacción ante posibles interrupciones de sus servicios para proteger los procesos considerados críticos ante la ocurrencia de fallos o desastres”¹.

En otras palabras, cuando hablamos de PCN, estamos hablando de lo que debemos hacer para asegurar la continuidad interrumpible de los servicios que brinda la institución educativa en caso de que ésta se viera sometida a una interrupción no deseada.

Los beneficios a los cuales se vería abogado las instituciones que lo han adoptado serían entre otros:

- Brindar continuamente los servicios que brinda la institución ante un desastre y/o minimizar el tiempo de recuperación de las operaciones normales a lo mínimo.
- Identificación proactiva de los impactos derivados de la interrupción operativa, en tal forma que se logre la reducción de aquellos riesgos que, en caso de materializarse las amenazas que les originan, pueden representar pérdidas ingentes de capital, bien por facturación fallida, por reposición de los daños causados, por pérdida de oportunidad de negocio, por reclamación de clientes, en el caso de la institución estos clientes son de dos

¹ ANTON, F. (2007) “El objetivo es proporcionar mecanismos de reacción ante posibles interrupciones de los servicios para proteger los procesos considerados críticos”. PLAN DE CONTINUIDAD DE NEGOCIOS, Rev. De Perspectiva Empresarial. 92 – 95.

tipos: cliente interno referido al estudiante, así como también personal docente y administrativo y cliente externo referido al padre de familia, por sanciones legales que vienen dadas por el Ministerio de Educación, etc.

- Ahorro de tiempo y dinero al afrontar y corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio, es decir, vendría dada por una respuesta efectiva a interrupciones.
- Mejora de la imagen y revalorización de la confianza en la institución educativa, está claro que esto permitiría la tranquilidad de la Comunidad, empleados, proveedores y clientes (estudiantes, docentes, personal administrativo y padres de familia) al mostrarles que se toman medidas diarias para garantizar la continuidad del negocio.
- Ventaja competitiva debido a la demostrada capacidad de mantener la entrega de servicios, permitiendo a los clientes comprometerse con la gestión educativa que se procura dentro de la institución.

1.2. Aprobación y comunicación del contenido del PCN

Los informes de la función de continuidad del negocio dependen de cómo está estructurada cada organización. Encontrar el lugar idóneo para la continuidad del negocio es un esfuerzo verdadero, el factor de éxito más importante, es que los programas de continuidad del negocio tengan el apoyo de la Gestión Directiva.

Un importante elemento al que hace frente una organización de educación, así como organizaciones e instituciones de todas las clases, es acerca de cómo los individuos obtendrán el conocimiento sobre la continuidad del negocio para apoyar un programa de esta índole.

Como primer paso se requiere la definición de una política general que garantice que todas las actividades serán diseñadas e implementadas bajo unos criterios comunes. La política debe definir el alcance, los principios y los recursos dedicados a la gestión de la continuidad. Consideremos pertinente señalar que esta política, que apuntan a la Continuidad del Negocio, ha de ser tratadas como una continuidad de las políticas que vienen ya expuestas o creadas en la institución misma.

Una vez definidas las líneas generales, se requiere proceder a la elaboración del programa de gestión de la continuidad. Este deberá asignar responsabilidades, para la identificación, minimización o eliminación de riesgos, y gestionar su actualización, promoción y mantenimiento del plan

El propósito de esta etapa es lograr además que los directivos de la institución se concienticen de la importancia del PCN, aprobar el desarrollo del mismo y por ende todo el personal con el fin de comunicar el desarrollo del mismo.

A continuación, el formato para efectuar este comunicado:

CIRCULAR

Para: Personal administrativo, docente y de servicio

De: Rectorado

Asunto: Plan de Continuidad de Negocio en el Ámbito Educativo

Fecha: 20 de octubre del 2009

A través de la presente se pone en conocimiento de todo el personal de la Institución de la Implementación a cargo del Ing. Patricio Martínez B. del Plan de Continuidad de Negocio en el Ámbito Educativo, que a palabras del suscrito es para conservar los Servicios de la Obra Educativa en caso de algún tipo de emergencia, riesgo o similares.

Sin otro particular

Atentamente,

Sor Zoila Pacheco

1.3. Definición de políticas en la planeación del Plan de Continuidad de Negocios (PCN).

Los requerimientos mínimos que se contemplan en la institución educativa para el desarrollo de nuestro PCN como políticas requeridas son:

- Se está desarrollando el presente Plan de Continuidad de Negocios como respaldo para el buen desenvolvimiento de la Institución. Si la Institución tuviera un PCN que contemple todas las actividades del negocio, hubiésemos revisado el plan por completo ya que el objetivo de esta revisión es determinar si cumple efectivamente o no con las necesidades proyectadas del negocio. Verificaríamos la fecha de generación del PCN y la fecha de la última actualización. Sin embargo, la Obra Educativa no posee este enfoque por lo que a continuación se exponen las otras políticas de acción requeridas.
- Se está llevando una evaluación de los riesgos para determinar los requerimientos del PCN. Por esta razón, en la política del PCN construimos una estructura reconocible e incluimos una sección detallada de los incidentes y riesgos que cubra todas las actividades claves del negocio. El plan contempla y documenta la estrategia de recuperación del rango

completo de procesos de negocio, incluyendo los sistemas IT, comunicaciones, información del negocio, niveles del servicio al cliente, relaciones públicas, etc.

- Existe una fase de recuperación del desastre con instrucciones al equipo que se encarga de la recuperación del desastre. En esta política se incluyen las instrucciones a seguir durante el proceso de recuperación del negocio, evaluadas y priorizadas, las actividades de recuperación, notificación y reporte y la organización del proyecto.
- Otras políticas para llevar a cabo el proyecto del PCN son: el aumento en los últimos años de la dependencia del instituto educativo de los sistemas de información computarizados.
- Aumento de la probabilidad de garantías inadecuadas de seguridad de la información e IT
- Aumento del reconocimiento del impacto que un incidente serio puede tener en el colegio
- Necesidad de establecer un proceso formal a seguir cuando ocurre un desastre.
- Necesidad de desarrollar un backups y estrategias de recuperación efectivas para mitigar el impacto de eventos disruptivos.
- Intención de reducir los costos o las pérdidas que surgen de los incidentes serios.
- Se realizará como políticas de acción, un testeo periódico y se simulará el entorno para asegurar que puede ser implementado en situaciones de emergencia y que los Servicios y el Personal entiendan como deben ser ejecutados.
- Todo el personal estará consciente del PCN y principalmente de su propio rol dentro del mismo.
- El Plan de Continuidad de Negocios se mantendrá actualizado de manera que tendremos en cuenta las circunstancias cambiantes.

La declaración de estas políticas será comunicada a todos los dueños de los Servicios de la Institución y al personal como tal, esto como parte del proceso de gestión de la política de la seguridad de la información.

1.4. Presupuesto preliminar para el desarrollo del PCN

Cada fase del proceso PCN que incurre en un costo requiere que se prepare y se apruebe el presupuesto. La fase de preparación para una posible emergencia del proceso PCN involucra la identificación e implementación de las estrategias para el backups y la recuperación de los archivos de datos o una parte del proceso de negocio. Es inevitable que estos procesos de backups y recuperación impliquen costos adicionales. Las partes críticas del proceso de negocio como los sistemas IT pueden requerir la implementación de estrategias particulares de backups costosas.

Si los costos son significativos deben ser aprobados con el detalle del presupuesto en forma separada del establecimiento y los costos de funcionamiento y mantenimiento.

Esta sección del PCN contiene una lista de las actividades de la fase de testing y el costo incurrido en cada una. Para cubrir los costos incorporados en el proceso normal del presupuesto de la organización se realiza lo siguiente:

En primer término se da a conocer al Servicio Directivo de la necesidad de implementar el PCN, en este Servicio se revisa su aplicabilidad y funcionalidad, este aprueba, así como también el costo en el que incurre este proceso. Inmediatamente, se hace llegar la aprobación del PCN y su costo al Servicio de Mantenimiento y Reparaciones, estos revisan el presupuesto y piden al Servicio de Colecturía el desembolso de lo requerido para cubrirlo.

A medida que el proyecto avance, serán necesarios otros presupuestos adicionales, relacionados con el análisis financiero de los costos de adopción de diversas estrategias de recuperación. Por lo que deberá ser considerado el Recurso Humano para la gestión del proyecto. Herramientas de planificación del PCN, plantillas y materiales de referencia. A continuación exponemos un primer acercamiento del valor inicial de cada uno de los servicios de la Institución, cuyos valores son expuestos basados en las entrevistas a los administradores y cifras dadas por facturas obtenidas que no se quiere hacer de carácter público:

PRESUPUESTO PRELIMINAR DEL SERVICIO DE ADMISIÓN		
RECURSOS	DESCRIPCIÓN	COSTO (\$)
1. Materiales	<ul style="list-style-type: none"> • Suministros de oficina: • Muebles y Enseres. • Archivo Muerto 	1200,00
	<ul style="list-style-type: none"> • Tecnológicos: - 1 Computadora - 1 Impresora HP Laser - 1 Impresora Matricial - Máquina de Escribir - Regulador de voltaje - Internet - Sistema de notas - Servicio telefónico 	2020,00
2. Humanos	<ul style="list-style-type: none"> - ADP - Auxiliar de Contabilidad 	800,00
SUBTOTAL		4020,00
Imprevistos (%5)		201,00
Total del presupuesto preliminar		3819,00

PRESUPUESTO PRELIMINAR DEL SERVICIO DE COLECTURIA		
RECURSOS	DESCRIPCIÓN	COSTO (\$)

1. Materiales	<ul style="list-style-type: none"> • Suministros de oficina: Se incluye al material del desván propio del servicio. • Muebles y Enseres. 	6400,00
	<ul style="list-style-type: none"> • Tecnológicos: <ul style="list-style-type: none"> - 2 Computadoras - 1 Impresora HP Laser - 1 Impresora Matricial - Regulador de voltaje y UPS - Internet - Servicio telefónico 	1060,00
2. Humanos	<ul style="list-style-type: none"> - ADP - Auxiliar de Contabilidad 	800,00
SUBTOTAL		8260,00
Imprevistos (%5)		413,00
Total del presupuesto preliminar		7847,00

PRESUPUESTO PRELIMINAR DEL SERVICIO DE MANTENIMIENTO Y REPARACIONES		
RECURSOS	DESCRIPCIÓN	COSTO (\$)
1. Materiales	<ul style="list-style-type: none"> • Suministros de oficina • Muebles y Enseres. 	2200,00
	<ul style="list-style-type: none"> • Tecnológicos: <ul style="list-style-type: none"> - Servidor HP Proliant ML 150G6 - 24 Estaciones de trabajo - 1 Impresora Matricial - DSL Wireless HUAWEI Echolife HG520s - Switch 3COM Super Stack 3 3C16471 - Regulador de voltaje y UPS - Internet - Servicio telefónico 	10179,00
2. Humanos	<ul style="list-style-type: none"> - ADP - Asesor Técnico 	1100,00
SUBTOTAL		13479,00
Imprevistos (%5)		673,95

Total del presupuesto preliminar	12805,05
---	-----------------

PRESUPUESTO PRELIMINAR DEL SERVICIO ACADÉMICO		
RECURSOS	DESCRIPCIÓN	COSTO (\$)
1. Materiales	<ul style="list-style-type: none"> • <i>Suministros de oficina</i> • <i>Muebles y Enseres.</i> 	750,00
	<ul style="list-style-type: none"> • Tecnológicos: <ul style="list-style-type: none"> - 1 Computador personal - Información impresa y respaldo - Regulador de voltaje - Internet - Servicio telefónico 	2420,00
2. Humanos	<ul style="list-style-type: none"> - ADP - Subdirección 	1400,00
SUBTOTAL		4570,00
Imprevistos (%5)		228,50
Total del presupuesto preliminar		4341,50

PRESUPUESTO PRELIMINAR DEL SERVICIO DE GESTIÓN HUMANA		
RECURSOS	DESCRIPCIÓN	COSTO (\$)
1. Materiales	<ul style="list-style-type: none"> • <i>Suministros de oficina</i> • <i>Muebles y Enseres.</i> 	1350,00
	<ul style="list-style-type: none"> • Tecnológicos: <ul style="list-style-type: none"> - 3 Computadoras personales - Impresora Samsung laser - Escáner - Regulador de voltaje - Internet - Servicio telefónico 	1540,00
2. Humanos	<ul style="list-style-type: none"> - ADP - Asesor técnico 	1200,00

SUBTOTAL	4090,00
Imprevistos (%5)	204,50
Total del presupuesto preliminar	3885,50

PRESUPUESTO PRELIMINAR DEL SERVICIO DE AUDITORÍA		
RECURSOS	DESCRIPCIÓN	COSTO (\$)
1. Materiales	<ul style="list-style-type: none"> • <i>Suministros de oficina</i> • <i>Muebles y Enseres.</i> 	700,00
	<ul style="list-style-type: none"> • Tecnológicos: <ul style="list-style-type: none"> - Servidor DELL Power Edge SC 440 - Backups – UPS RS 1200 APC - Impresora HP Laser P2015 dn - Kypus Server Appliance - Router EDIMAX EW 7209 APg - 10 Estaciones de trabajo Vía Samuel 2 	6050,00
2. Humanos	<ul style="list-style-type: none"> - ADP - Lider auditor 	1100,00
SUBTOTAL		7850,00
Imprevistos (%5)		392,50
Total del presupuesto preliminar		7457,50

1.5. Organización del equipo del proyecto

Se identificará al equipo del proyecto en orden de importancia para la institución, así esta quedaría definida de la siguiente forma:

1. Inicio y administración del proyecto. El papel de los profesionales de la continuidad del negocio en esta etapa es conducir a los patrocinadores de proyecto (en nuestro estudio a la Gestión Directiva) para definir objetivos, políticas y factores críticos del éxito; coordinar y administrar el proyecto de Continuidad del Negocio; supervisar el proceso de Continuidad del Negocio a través de una metodología de control y administración del cambio; defender el proceso ante la gerencia y el personal; desarrollar el plan y presupuesto del proyecto; definir y recomendar a la estructura y administración e implementar el proceso de planeación de Continuidad del Negocio. Equipo de la Alta Dirección.
2. Evaluación y control del riesgo. El rol en esta actividad, es identificar los riesgos potenciales en la organización; entender cómo reducir y atenuar estos riesgos; identificar si se requiere experiencia externa; identificar el grado de exposición de la organización; identificar las alternativas para la mitigación y/o reducción del riesgo; conforme a la gerencia determinar los niveles aceptables de riesgo, documentar y presentar los resultados. Equipo de la Alta Dirección.
3. Análisis de impacto en el negocio: su papel en esta parte es identificar a expertos con amplios conocimientos de las funciones de las diversas áreas; identificar funciones, instalaciones, personal y tecnología de la organización; identificar y definir los criterios de criticidad y obtener la aprobación de la Gestión Directiva para los criterios definidos. Equipo de Gestión Humana.
4. Desarrollar las Estrategias de Continuidad del Negocio. El rol del profesional es analizar las alternativas disponibles, sus ventajas, desventajas y costos; identificar las estrategias viables de la recuperación para cada área funcional del negocio; consolidar las estrategias; desarrollar las estrategias de la unidad de negocio y obtener el compromiso de la gerencia para las estrategias desarrolladas. Equipo de Colecturía.
5. Respuesta y operación de emergencias. Identificar los tipos potenciales de respuesta a emergencias; verificar la existencia y ubicación de los procedimientos para respuesta a emergencias, recomendar el desarrollo de tales procedimientos donde no existan; integrar los procedimientos de Continuidad del Negocio y Recuperación de Desastres mediante la respuesta a emergencias y procedimientos escalonados; identificar los controles y ordenes necesarias para el manejo de una emergencia; recomendar el desarrollo de los procedimientos de control para definir roles, autoridades y procesos de comunicación

para el manejo de emergencias y asegurar que los procedimientos de respuesta a emergencias cumplan los requisitos de las autoridades. Equipo de Mantenimiento y Reparaciones.

6. Desarrollar e implementar los Planes de Continuidad del Negocio. Identificar la metodología del planeación, organización, dirección de esfuerzos y necesidades del personal; controlar el proceso del planeación y producir, implementar, probar y mantener el plan. Equipo de la Alta Dirección.
7. Programas y entrenamiento de concientización. El papel del profesional es establecer objetivos y componentes del programa de concientización y capacitación; identificar los requisitos de capacitación para las áreas funcionales; desarrollar la metodología del concientización y capacitación; adquirir y desarrollar herramientas para capacitación y concientización e identificar las oportunidades de capacitación y concientización externas o alternativas. Equipo de Gestión Humana.
8. Mantener y aplicar los planes de continuidad del negocio. Planear, coordinar y facilitar las prácticas de los planes; evaluar y documentar los resultados de los ejercicios; actualizar el plan; reportar los resultados y evaluaciones a la gerencia; coordinar el plan de mantenimiento y asistir en el establecimiento de un programa de auditoría del plan de continuidad del negocio. Equipo de Auditoría.
9. Comunicaciones en la crisis. Establecer programas para comunicaciones proactivas en las crisis; establecer la coordinación de la comunicación de la crisis con las agencias externas; establecer la coordinación necesaria de la comunicación de la crisis con los grupos relevantes; y establecer y probar los medios de comunicación entre la institución y sus unidades de negocio. Equipo de Auditoría.
10. Coordinación con agencias externas. Identificar y establecer los procedimientos de enlace para el manejo de emergencias; coordinar la administración de emergencias con las agencias externas; y mantener actualizado su conocimiento sobre leyes y regulaciones referentes a la administración de emergencias. Equipo de Alta Dirección.

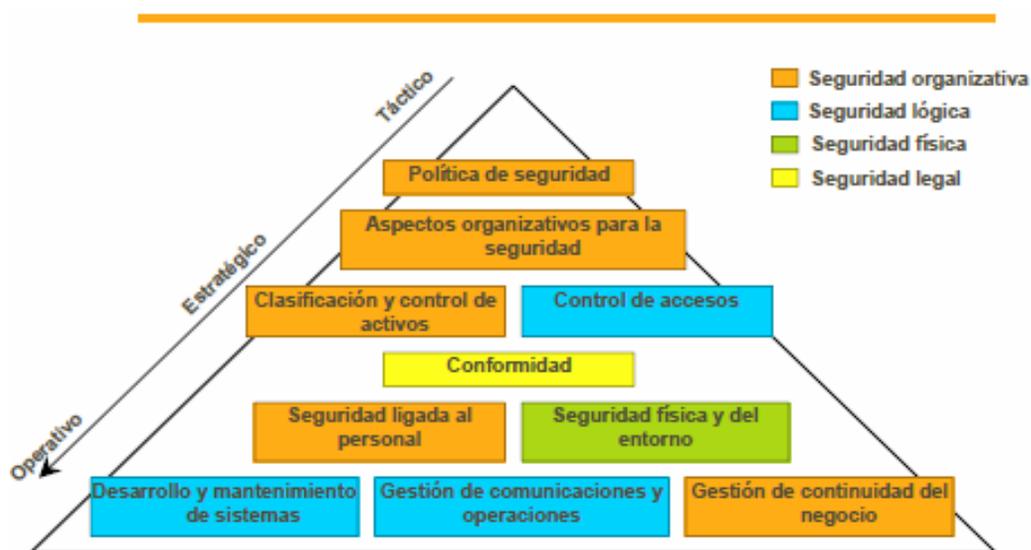
2. Identificación de los Servicios Críticos de la Institución

La Obra Educativa “Nuestra Señora del Rosario” en su contexto, viene trabajando manteniendo en su prioridad la certificación a la Norma ISO 9001 – 2008, desde hace 2 años, con auspicio de la empresa QUALY PLUS, para certificar a través de la empresa auditora ICONTEC.

El PCN, está orientada a través de la Norma ISO 27002:2005 (Véase Anexo 1) “la misma que aún no posee ningún tipo de certificación, únicamente constituyen recomendaciones y no es necesario aplicar la totalidad de sus controles, sino adaptarlos a la organización”²,

Sin embargo, el interés de la utilidad de la ISO 27002:2005 para el desarrollo del presente proyecto, está en definir claramente los once dominios básicos y particularmente el dominio 10 que se refiere a Gestión de Continuidad del Negocio, que son útiles en un PCN y que servirán como normas bases para la identificación de los servicios críticos de la institución.

Luego del respectivo análisis de los servicios que brinda la institución teniendo en cuenta lo de la norma 27002 y en base al siguiente esquema: se han identificado los siguientes servicios críticos.



Tomado de TI y Continuidad de Negocio, www.borrmart.es/index.php.

Lo expuesto engloba seguridad organizativa, seguridad lógica, seguridad física, seguridad legal, desde lo táctico, hacia lo estratégico y finalmente hacia lo operativo.

²ARGENTERO, C. (2006, septiembre): ISO 17799. La seguridad informática no es un producto sino un proceso (en línea). Córdoba. Disponible en: <http://www.deobit.com>

Entre las razones que hemos utilizado para la identificación de los Servicios Críticos están básicamente en definir aquellos Servicios que al caer podrían sufrir graves consecuencias al desenvolvimiento normal de la institución. Así mismo el tiempo dentro del cual el proceso de la institución podría ser restaurado dentro de niveles aceptables de capacidades operacionales para minimizar el impacto de la caída. Los Servicios que brinda la institución son:

2.1. Servicio Académico

CARACTERIZACIÓN DEL SERVICIO

Objetivo:

Direccionar el servicio de enseñanza aprendizaje mediante la planificación, ejecución, evaluación y mejora continua; asegurando que todo trabajo educativo sea realizado como misión profética para garantizar una formación integral de los educandos en sus tres dimensiones: cognitivo, praxitivo y afectivo.

Alcance:

Planificar el proceso académico, finalmente, evaluación y la mejora continua.

Entradas:

Acuerdos legales de funcionamiento, Reglamento General de la Ley de Educación, modelo pedagógico, proyecto educativo congregacional, planificación del formato del proceso académico, reporte y seguimiento de casos, recomendaciones y sugerencias, listado de estudiantes nuevos, matrícula condicionada, leccionario, listado para estudiantes con matrícula condicionada o negada, transferencia y epicrisis, finalmente horarios.

Proveedores:

Ministerio de Educación, Dirección Provincial de Educación, autores del modelo pedagógico: hermanos Zubiria Samber, Congregación de Hermanas Dominicas, Ministerio de Inclusión Económica y Social, Proceso de Psicología, Proceso de Admisión, Proceso de Disciplina y Proceso de Salud.

Funciones:

El Servicio Académico se maneja a través del sistema operativo Windows XP en el que deposita a través de carpetas individuales las aplicaciones y datos que se requieren para su función:

1. Guiar e implementar la planificación Plan Curricular Institucional (PCI), Plan de Unidad Didáctica (PUD) y Plan Semanal de Clase.

2. Aplicación de documentación macro y micro curricular: Proyecto Educativo Institucional (PEI), PCI, PUD, Plan Semanal de Clases, Registro de Calificaciones del Docente, Cuadro de Ingreso de Calificaciones.
3. Ejecución de la planificación
4. Revisión y análisis de documentación macro y micro curricular
5. Análisis del proceso de enseñanza – aprendizaje.
6. Impulsar el mejoramiento continuo del proceso enseñanza – aprendizaje.

La mayor parte de la información está elaborada en la aplicación Microsoft Word, y se complementa en Excel la elaboración de los procesos de seguimiento, sin embargo, muchos de estos no están protegidos a través de contraseñas que es tarea de nuestro PCN. Toda la información esta almacenada en el Disco Duro de la computadora, tampoco se ha creado medios de respaldo, ya que no se realizan backups continuos para su protección y este ordenador únicamente cuenta con un regulador de voltaje que tampoco garantiza que en caso de corte de luz no se pierda la información importante o que acarree daños directos a la funcionalidad del hardware. El acceso está restringido únicamente a la Vicerrectora de la Institución, pero ella lo facilita a los colegas sin restricción alguna.

Salidas:

Distributivo de trabajo, plan semanal de clase, cuadro de ingreso de calificaciones, matrícula condicionada, leccionario, reporte y seguimiento de casos, cuadro de ingreso de calificaciones, entrevista académica al personal nuevo, oficios, PEI, documentos del proceso académico, indicadores y planes de mejora.

Clientes:

Proceso de disciplina, de ejecución y evaluación, documentación, comité de calidad y mejora, proceso de psicología, de gestión humana y proceso de comisiones.

Documentos internos y externos:

Acuerdos legales de funcionamiento, Reglamento General de la Ley de Educación, Modelo Pedagógico, Proyecto Educativo Congregacional.

Registros generados:

- PCI de pre básica, básica y bachillerato R1.1-034 (Registro, número de servicio, número de ejecución, número de formato de registro)
- PUD R1.1-04
- Plan de Área R1.1-05
- Formato de recepción de documentos R1.1-12
- Distributivo de trabajo R1.1-14
- Plan Semanal de Clases R1.1-18
- Ficha académica R1.2-17

- Formato de calificaciones del docente R1.2-03
- Formato de evaluación al estudiante R1.2-04
- Hoja de observaciones de clase R1.2-05
- Acta de área R1.2-08
- Encuesta académica R1.2-15
- Informe reunión Padres de familia R1.2-18

Seguimiento y medición:

- 70 % de docentes que trabajan con una carga horaria de acuerdo a su especialidad y 30 % de docentes que trabajan con materias afines
- 85% de estudiantes con notas superiores a catorce (14);
- 85 % de profesores excelentes en el desempeño académico aplicando pedagogía conceptual

Recursos:

Talento humano completo, equipos tecnológicos, planta física e infraestructura adecuada y archivos correspondientes al proceso.

Procesos de apoyo:

1. Admisión
2. Psicología
3. Disciplina
4. Gestión Humana
5. Salud
6. Comisiones

Requisitos a cumplir:

Requisitos de la Ley de Educación Requisitos de la norma ISO 9001-2008, (Véase en Anexo 2) requisitos de la congregación de hermanas Dominicanas y requisitos del modelo pedagógico

2.2. Servicio Gestión Humana

CARACTERIZACIÓN DEL SERVICIO

Objetivo:

El Servicio de Gestión Humana logrará que el personal que integra la OBRA EDUCATIVA “NUESTRA SEÑORA DEL ROSARIO”, desarrolle, valore, evalúe, y fortalezca su Calidad Humana para conservar la Identidad Institucional Rosarista, cumpliendo con los perfiles en el ámbito personal, esto es en lo moral y espiritual, y en el ámbito profesional en lo intelectual.

Alcance:

El Servicio interactúa directamente con la gestión académica, pastoral, psicológica y administrativa, cuando existe la necesidad de contratar personal que cumpla con los perfiles establecidos por la institución, se realiza la búsqueda del personal, la selección, inducción, capacitación, evaluación, motivación y salida de personal.

Entradas:

Código del Trabajo, Ley de Educación, Contrato de Trabajo, Oficios y Entrevista Académica.

Proveedores:

Ministerio de Educación, Ministerio de Trabajo y el Proceso Académico.

Funciones:

El Servicio de Gestión Humana también está trabajando sobre el Sistema Operativo Windows XP, y tomando como base del manejo de sus aplicaciones Microsoft Word, las funciones a su cargo son:

1. Seleccionar el personal, integrándolo a través de un proceso de inducción.
2. Capacitar y evaluar al nuevo personal en su desempeño. Se gestionará en una continua motivación.
3. Revisar el cumplimiento de los requisitos de selección y contratación previos, y en idéntica forma conocer los lineamientos de la institución.
4. Capacitar al personal a través de un cronograma y la evaluación del desempeño a lo largo del año lectivo.
5. Asignar para la motivación espacios de integración y entrevistas personalizadas.
6. Realizar la selección de personal en coordinación con el proceso académico y rectorado.
7. Observar el desempeño favorable del personal a lo largo del año lectivo
8. Buscar mecanismos de satisfacción de las expectativas identificadas en el personal.
9. Impulsar la mejora continua del personal de la Obra Educativa.

La comunicación entre los diferentes departamentos que se encuentran a su cargo se da a través de redes inalámbricas sujetas por un Router D – link 300, en un total de 4 estaciones inalámbricas y se suman dos estaciones alámbricas a través de un cable de red tipo Coaxial Categoría 5, con conectores RJ – 45. Cada una de las estaciones tiene un control central para registro de dominios aplicados recientemente a través del programa Kerios, en términos generales este programa está especialmente enfocado para empresas de tamaño medio, en las que ofrece un control total sobre el tráfico en la red y una protección eficaz en múltiples máquinas, incluso si usan Linux, Mac OS, Unix o AS400. Soporta cualquier tipo de conexión, ya sea cable, ADSL, Wireless, módem, etc. Se adapta a cualquier protocolo soportando: IPSEC, H.323, NetMeeting, Net2Phone, WebPhone, UnixTalk, RealAudio, RealVideo, ICA Winframe, IRC, FTP, HTTP, Telnet, PPTP, Traceroute, Ping, cuseeme, daytime, discard, dns, echo, finger, gopher, https, imap3, imap4, ipr, IPX overIP, netstat, nntp, ntp, ping, pop3, radius, wais, rcp, rlogin, rsh, smtp, snmp, ssh, systat, tacacs, uucpover IP, whois, xtacacs, etc.

Además en este Servicio cuentan con reguladores de voltaje, pero ninguna de ellas tiene un UPS de respaldo, por lo que cualquier alteración en la normal alimentación del fluido eléctrico conllevaría graves pérdidas. Sin embargo, un punto de apoyo para evitar las pérdidas expuestas está en la continua elaboración de backups a través de un Disco Duro externo, marca LG, de 320 GB que por hoy provee suficiente capacidad de almacenamiento. Cada una de las estaciones tiene un solo usuario o propietario para su acceso, sin embargo, únicamente dos estaciones tienen protección de contraseña, las otras carecen del mencionado servicio.

No se manejan programas de Bases de Datos y toda la información prácticamente depende únicamente de la computadora personal de cada usuario y aquella que se envía como respaldo al disco externo expuesto.

Salidas:

Personal competente, Documentos y Registros e Indicadores

Clientes:

Proceso académico, Representante de la Alta Dirección y Proceso de calidad.

Documentos Internos y Externos:

Documentos de la congregación, Ley de Educación, Manual de perfiles, Manual de funciones y el Código de trabajo.

Requisitos generados:

- Manual de perfiles (R.11.O1)
- Solicitud de empleo (R.11.O2)
- Formulario de inducción (R.11.O3)
- Evaluación del desempeño (R.11.O4)

- Hoja de ruta de salida (R.11.O5)
- Plan anual de capacitación (R.11.O6)
- Evaluación de la capacitación (R. 11. 07)
- Informe del jefe directo(R.11.O8)

Seguimiento y medición:

- 100 % de hora persona por capacitación
- 100 % de hora eficaces de entrenamiento

Recursos:

Personal completo, archivo del proceso y finalmente equipos tecnológicos.

Procesos de apoyo:

1. Proceso de Adquisiciones
2. Presupuestaria
3. Proceso de Mantenimiento
4. Proceso de Salud y Seguridad

Requisitos a cumplir:

Requisitos de NTC ISO 9001: 2008, Requisitos de la Congregación, Requisitos de la Ley General de Educación y Requisitos del Código de Trabajo

2.3. Servicio de Admisión

CARACTERIZACIÓN DEL SERVICIO

Objetivo:

El Servicio de Admisión da a conocer a todos los Padres de Familia de niños y jóvenes, nacionales, y extranjeros sin distinción de religión, comprendidos en edad escolar, que desean ingresar y permanecer en la Obra Educativa “Nuestra Señora del Rosario”, que deben proporcionar la información individual necesaria para los Procesos de: Salud y Seguridad, Psicología y Bienestar Estudiantil, Disciplina, Alta Dirección y Pastoral, para su ingreso en la Institución.

Alcance:

El Servicio de Admisión informa a través de su URL: www.colrosario.edu.ec, sobre los servicios educativos que brinda la Institución. Da a conocer los requisitos para la admisión de estudiantes nuevos mediante informativos impresos, finalmente matricula estudiantes nuevos y antiguos basándose en el Reglamento General de Educación e Interno de la Institución, contribuyendo a que estudiantes y padres de familia acepten los principios de formación que ofrece el plantel. Inicio: Planificación del proceso de Admisión, Final: Matriculación de l@s estudiantes.

Entradas:

Fe de bautismo, partida de nacimiento, pases de año y matrículas, certificado médico, comprobante bancario, reglamento general de la Ley General de Educación, autorización de matrícula, listado de orientación vocacional y listado de estudiantes con problemas disciplinarios.

Proveedores:

Padres de familia, M.E.C. Proceso de Disciplina, Proceso de Psicología y Bienestar Estudiantil.

Funciones:

Al igual que los otros servicios en estudio, el Servicio de Admisión tiene como base el sistema operativo Windows XP:

1. Dar a conocer los servicios educativos y la dirección electrónica de la Institución al Padre de Familia.
2. Indicar requisitos a Padres de Familia para el proceso de inscripción y matriculación
3. Entregar documento que conste los servicios educativos
4. Entregar el informativo de inscripción y de matrícula
5. Inscribir y matricular a los estudiantes para el nuevo año lectivo
6. Buscar nuevos mecanismos para publicitar a la Obra Educativa con el fin de llegar al mayor número de estudiantes y padres de familia en general.
7. Ingreso de calificaciones por parte del personal docente.

Los datos sobre la información orientada a los padres de familia se elabora en la aplicación Microsoft Power Point, en lo relacionado a los requisitos sobre los procesos de inscripción a través del internet, la Institución cuenta con su propia página WEB elaborada por LinkSphere, cuya actualización y mantenimiento se realiza anualmente.

En lo referente a la inscripción, matriculación, ingreso de notas por parte del personal docente, la Obra Educativa cuenta con su propio programa generado en Visual Fox Pro y se le conoce con el nombre de Sistema de Notas del colegio “Nuestra Señora del Rosario” , esto ha permitido agilizar todos los procesos de trabajo mencionados previamente.

La comunicación con los servidores principales de la Institución se da a través un router D – link 5100 a donde se envía la información que proviene de este programa, además cuenta con un Disco Duro externo Samsung para respaldar la información de manejo. Cuenta con contraseñas de seguridad para permitir el acceso únicamente al personal del Servicio. Estas contraseñas son guardadas en el disco Samsung, pero no se tiene un medio como Lock Note para respaldo de las mismas, este será implementado en conjunto con el PCN.

La computadora de este Servicio cuenta con un UPS de auxilio, en tal medida que cualquier corte del normal flujo de la electricidad da un tiempo aproximado de 15 minutos para respaldar y guardar.

Salidas:

Documentos y registros e indicadores.

Clientes:

Padres de familia, Comité de calidad, Proceso de disciplina, Proceso de salud y seguridad, Proceso académico, Proceso pastoral, Proceso de adquisiciones y presupuesto, Proceso de psicología y bienestar estudiantil.

Documentos Internos y Externos:

Ley de Educación y Reglamento Interno de la Institución.

Registros generados:

- Indicadores
- Informativo de inscripciones
- Listado de estudiantes del año que termina
- Informativo de matrículas
- Listado de estudiantes para el curso de nivelación
- Carpeta institucional
- Hoja de matrícula
- Listado de estudiantes para el año nuevo

- Listados de estudiantes que no poseen fe de bautismo

Seguimiento y medición:

- % tasa de crecimiento estudiantil
- % de estudiantes que se inscriben y matriculan
- % de estudiantes antiguos que no se matriculan
- % de causas de no matriculación

Recursos:

Estudiantes nuevos y antiguos, archivo del proceso, equipos tecnológicos.

Procesos de apoyo:

1. Alta Dirección
2. Proceso Académico
3. Proceso de Psicología y Bienestar Estudiantil
4. Proceso de Disciplina

Requisitos a cumplir:

Requisitos de la ISO 9001: 2008, Requisitos de la Congregación y Requisitos de la Ley General de Educación.

2.4. Servicio de Mantenimiento y Reparaciones.

CARACTERIZACIÓN DEL SERVICIO

Objetivo:

Mantener funcionando la infraestructura necesaria para lograr la conformidad con los requisitos del producto de la Comunidad Educativa.

Alcance:

Este Servicio implica el correcto funcionamiento y estado de: edificios, equipos para los procesos del Sistema de Gestión de Calidad, laboratorios y departamentos (hardware); y servicio de transporte de los estudiantes.

Entradas:

Norma ISO, permiso de funcionamiento y derecho y obligaciones de niños y adolescentes.

Proveedores:

Tanto la Norma ISO, como la Empresa Metropolitana de Servicio y Administración del Transporte (EMSAT).

Funciones:

1. Idear estrategias de mantenimiento institucional que vayan acorde a las salidas presupuestarias de la congregación.
2. Atender las necesidades que se presenten en la infraestructura de la institución sean por factores internos y externos durante el transcurso de año lectivo 2009-2010
3. Debilidades y fortalezas encontradas en proceso de mantenimiento y reparaciones, para continuar el buen desempeño del sistema.
4. Impulsar el correcto y eficaz desarrollo de las buenas estrategias aplicadas en el proceso.

Para contar con un apoyo descriptivo de las funciones, se utiliza un computador personal Pentium IV, con sistema operativo Windows XP, pero este Servicio además mantiene los servidores que son descritos posteriormente, pero que es pertinente señalar que cuentan con Sistema Operativo Windows Server 2003 y Linux. También utilizan las aplicaciones de Microsoft Office, particularmente Word y Excel. Cuentan además con sistemas de energía ininterrumpible (UPS) de respaldo para evitar los cortes repentinos de luz. El acceso a los servidores está restringido a un solo usuario, sin acceso a otros, cualquier necesidad en los mismos requiere de una contraseña específica que la conoce exclusivamente el administrador.

Salidas:

Únicamente lo referente al Comité de Calidad.

Clientes:

Padres de familia y estudiantes.

Documentos Internos y Externos:

- Doc. Bitácora de utilización del equipo
- Doc. Notificación del daño
- Doc. Acta de entrega y recepción
- Doc. Orden de reparación
- Doc. Notificación del daño de edificios
- Doc. Orden de reparación edificios
- Doc. Incumplimiento de las normas de seguridad del transporte
- Doc. Proforma de servicio
- Doc. Norma ISO
- Doc. Permiso de funcionamiento de la Empresa Metropolitana de Servicios y Administración del Transporte (EMSAT)
- Doc. Ley de Educación
- Doc. Código de la Niñez

Registros generados:

- Bitácora de utilización del equipo R15-03
- Notificación del daño R15-04
- Acta de entrega y recepción R15 -05
- Orden de reparación R15-07
- Notificación del daño de edificios R15-09
- Orden de reparación edificios R15-10
- Doc. Incumplimiento de las normas de seguridad del transporte R15-11

Seguimiento y Medición:

- % de máquinas averiadas trimestralmente.
- % de notificación del bien material dañado u obsoleto anualmente.
- % de vehículos en buen estado trimestralmente.

Recursos:

Presupuesto, equipos tecnológicos y personal docente calificado.

Procesos de Apoyo:

Proceso de adquisición

Requisitos a cumplir:

Requisitos congregacionales, requisitos de la norma ISO 9001-2008, requisitos de la ley de tránsito y requisitos a la Ley de Educación.

2.5. Servicio de Auditoría

Inicialmente, en el análisis del presente proyecto, este proceso no se había considerado, pero en vista del delicado trabajo que cumplen los auditores en la Institución, consideramos pertinente el uso del mismo para el desarrollo del proyecto, es por eso que este es parte de los Servicios Críticos de la Obra Educativa, a continuación, al igual que en los otros procesos, exponemos sus características para justificar su uso:

CARACTERIZACIÓN DEL SERVICIO

Objetivo:

Definir las actividades y responsabilidades a seguir para auditar los procesos de la organización y poder establecer si el sistema de gestión de calidad está conforme con los requisitos de la norma internacional de la ISO 9001 – 2008.

Alcance:

Inicia en el auditor líder y finaliza con la entrega del Informe Final de Auditoría.

Entradas:

Ministerio de Educación, leyes del estado, las normas ISO y el proceso de Gestión Directiva.

Proveedores:

Proceso de Gestión de Calidad.

Funciones:

El lugar de trabajo del Servicio de Auditoría, es el aula de Contabilidad, donde se cuenta con las computadoras personales más actualizadas. Las funciones que cumple este Servicio son:

1. Liderar la planeación de las auditorías internas en la institución, de acuerdo con los criterios y el alcance establecidos por la alta dirección.
2. Ejecutar las auditorías planificadas de conformidad con los requerimientos de la organización.
3. Evidenciar la funcionalidad de los procesos a través del procedimiento documentado.

4. Informar los resultados de las auditorías a la Gestión Directiva para el desarrollo de las auditorías de seguimiento.

Su funcionalidad se da a través del Sistema Operativo Windows XP, pero interconectadas a través de redes inalámbricas para el intercambio de información, datos u otros archivos. Utilizan en idéntica manera Microsoft Word para la construcción de sus planeaciones y se apoyan en otras aplicaciones del mismo Office. La información relevante se almacena en otro servidor, cuyas características son descritas posteriormente. Este servidor cuenta con el apoyo de la Curia Diocesana de la ciudad de Quito, desde donde se realiza un control de seguimiento de la integridad del mismo, para impedir la instalación de otros programas que no sean previamente aprobados por la Curia. Plan Amanecer que es el convenio entre la Conferencia Episcopal y el Gobierno de España

Salidas:

Informe final de auditorías internas, y registro de control de producto no conforme, acciones correctivas y/o preventivas

Clientes:

Proceso de Gestión Directiva

Documentos Internos y Externos:

Norma ISO, Ley de Educación, Reglamento Interno y Lista de Auditores

Registros generados:

- Cronograma de auditorías
- Orden de auditorías
- Plan de auditorías
- Reporte de no conformidades
- Informe de auditoría
- Registro de control de producto no conforme, acciones correctivas y acciones preventivas
- Competencias y parámetros de evaluación de los auditores

Seguimiento y Medición:

Porcentaje de cumplimiento de los requisitos legales o regulatorios.

Recursos:

Equipo de auditores y documentos impresos

Procesos de Apoyo:

Gestión Directiva, Control de Documentos y Control de Producto no Conforme, acciones correctivas y/o preventivas.

Requisitos a cumplir:

Requisitos de la Norma ISO 9001-2008 y Requisitos del Sistema de Gestión de Calidad.

2.6. Servicio de Colecturía

CARACTERIZACIÓN DEL SERVICIO

Objetivo:

El servicio de colecturía tiene como responsabilidad asegurar el manejo adecuado de los recursos económicos de la institución, procurando que los estudiantes se encuentren al día en la cancelación de sus matriculas y pensiones. Así también velando por el interés económico de los docentes, personal administrativo y de servicio. Y también mantiene la infraestructura del colegio mediante la adquisición de diferentes bienes por medio de sus proveedores.

Alcance:

Inicia con el cliente interno y externo y finaliza con la entrega del Informe Final de Colecturía.

Funciones:

El Servicio de Colecturía cuenta con un único computador bajo el sistema operativo Windows XP, este departamento tiene como función:

Se comunica vía Internet al Banco Promérica a través del cual se realizan los depósitos de los sueldos de docentes, administradores y personal en general, razón por la cual para evitar cortes de luz cuenta con un UPS que se encarga de mantenerlo activo ante estos imprevistos, además cuenta con un ventilador permanente que le permite mantener al computador a temperaturas adecuadas de trabajo, evitando el calentamiento del procesador.

Para comunicaciones al personal utiliza la aplicación Word, pero para el manejo de la contabilidad cuenta con el programa T-MAX 2000 y Olimpo V7, además utiliza la aplicación Microsoft Excel para llevar las cuentas de caja chica.

Por otro lado, tiene una contraseña de acceso al computador pero únicamente a nivel de Sistema, y no a nivel de hardware. Cuenta con un sistema de red, a través de cable coaxial categoría 5 con conectores RJ – 45 para comunicarse directamente con el servidor central del departamento de computación. Esta contraseña ha sido la misma durante los últimos meses, a pesar del cambio de usuario.

Observación:

En vista de que este servicio no se contempla en la norma ISO 9001 – 2008, ya que los manejos financieros son de responsabilidad única de sus propietarios no se generan registros sobre el servicio. Pero en vista de su valor tecnológico y su relación directa con el PCN es prioritario su conocimiento y manejo.

3. Priorización de los Servicios Críticos

“Los Servicios son críticos para la continuidad del negocio dependiendo de las prioridades y características del sector y, en última instancia, de la empresa que se trate”³.

El enfoque de la ISO 27002 es seguridad en los sistemas de información y el enfoque del Objetivo de Control para la Tecnología de la Información (COBIT) es control de la información y de las tecnologías relacionadas, pero los dos tienen varias similitudes en el caso de continuidad de las operaciones. Esta estrategia deberá estar basada en los objetivos de la organización y en el nivel de riesgo que esté dispuesta a afrontar, ya que si bien coexisten es quién se encarga del manejo del sistema contable con la obtención de balances, control de cuentas de bancos, registros de avisos de entrada, roles de pago, sistemas de pensiones, presupuesto, elaboración del mismo, registro y control. No deja de ser relevante también toda la información que va direccionada hacia el estudiante, esto es a más de las matrículas como tal, sus notas, su asistencia a clases, el merecimiento de diplomas, la generación de planes de estudio mensual, semanal, mallas de trabajo, es decir, el control tecnológico de la vida estudiantil, aparte del mismo control sobre el desenvolvimiento de docentes, personal administrativo y de mantenimiento dentro de nuestra Institución.

Para complementar hacia donde se dirigen los procesos críticos del negocio debe considerarse como fundamental lo que se señala al mencionar: “... en última instancia, de la empresa de que se trate”. En este caso, el objetivo de la Institución en estudio señala: “Educar a la niñez y juventud en forma integral a través de un proceso humano – cristiano, científico, productivo e intercultural que responda a la realidad de su medio ambiente y contribuya activamente a la transformación de la sociedad”.⁴

Por ende, este es el servicio más importante, hacia allá se dirige los esfuerzos y en consecuencia esas son sus prioridades. Su prioridad es cumplir con las obligaciones que tienen con los estudiantes, es decir, si alguien necesita una educación de calidad, la Institución ha de estar disponible para ello. No se puede decir a los estudiantes que determinados temas no serán enfocados en vista de que no se ha preparado el material para ello o no se tiene el mismo. Se perdería confianza y clientes, además de la pérdida de prestigio, valor importantísimo, para mantener un PCN permanente.

Para la continuidad del negocio también resulta obvio que es responsabilidad de la Gestión Directiva el contar con una adecuada administración de la continuidad de negocios. Es importante

³ PEÑA IBARRA, J (2004): Planes de Contingencia, Recuperación de Desastres (en línea). México D.F. Disponible en: <http://www.ccisa.com.mx>

⁴ Obra Educativa “Nuestra Señora del Rosario”, Agenda 2009 – 2010, Objetivos de la Institución.

considerar que quienes ayudan a definir también son los administradores de cada servicio y la pregunta necesaria es ¿Qué pasa si tal o cual servicio dejan de funcionar?

Por lo expuesto, la información construida no tiene el mismo valor jerárquico, ya que la pérdida de datos en uno de los departamentos puede ser crucial, en tanto que, otro tipo de información perdida, en otro departamento, podría no alterar en mayor medida el desenvolvimiento del colegio, de allí que al aplicar este PCN es fundamental el tiempo de respuesta ante un incidente, y claro está los respaldos adecuados realizados en el transcurso del mismo. Para la priorización de los servicios se ha tomado en consideración la responsabilidad asignada a cada administrador de los Servicios, los mismos que han sido enfocados a través de entrevistas, obteniendo las siguientes observaciones, el modelo de entrevista a los administradores se encuentra en el Anexo 3:

Para la priorización de los servicios críticos en base a los resultados de las entrevistas a los ADP de Servicio y acorde a la experiencia que se ha adquirido en el desarrollo del proyecto, establecemos en primer término porqué el Servicio de Admisión es el más importante:

Para ello es prioritario recordar que la función básica de la Obra Educativa “Nuestra Señora del Rosario” tiene como Misión: “Ofrecer a la Comunidad Educativa una educación integral de calidad a la niñez y juventud , basada en: el amor, la exigencia, razonamiento crítico, principios evangélicos, congregacionales y científicos potenciando sus capacidades para la formación de seres humanos emprendedores que contribuyan al crecimiento de la sociedad”

Por lo revisado, la priorización de los Servicios sería:

- **Servicio de Admisión**, en vista de la infabilidad que debe mantener en lo relacionado a la Disponibilidad e Integridad de la Información, así como también lo referente a la Confiabilidad del manejo de datos, el administrador del Servicio se encuentra en la obligación de conocer perfectamente el programa diseñado para su cargo, en este caso básicamente el Sistema de Notas “Nuestra Señora del Rosario”, cumplir con la obligación de mantener respaldos continuos de la información y aplicar un conjunto de contraseñas que impidan el acceso a personal no autorizado. Su violación, claro está, podría generar resultados falsos que causarían graves alteraciones a los estudiantes y a la calidad del colegio, en lo referente a su prestigio institucional. Además, este servicio maneja documentación de relevancia que son propiedad exclusiva de la Institución y otros que son entregados a los alumnos y alumnas para sus requerimientos particulares, esto es: Títulos de Bachiller, Actas de Grado, Pases de Año, documentos específicos de los estudiantes como partida de nacimiento, fe de bautizo, entre otros, que reflejen lo expuesto como seres humanos emprendedores que contribuyen al crecimiento de la sociedad. Esto marca el fundamento de haber sido asignado como Primer Servicio Crítico.
- **Servicio de Colecturía**, a este se añade como básico el hecho de considerar la Confidencialidad de la información, datos que son trascendentes únicamente para determinado grupo de personas, la Institución debe disponer de procedimientos que

garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de el colegio, tareas específicas que van relacionadas con el Sistema de Cobro de Pensiones, pago de sueldos al personal de la Institución, pago de haberes a los proveedores y cubrir lo relacionado al pago de impuestos. El administrador del Servicio debería establecer su propia contraseña sin dar lugar a la sospecha de la misma, evitando que se relacione con claves referentes a su familia u otro tipo de referencias personales, evitando ataques de diccionario o de fuerza bruta. Añadiendo a su Servicio un firewall que le permita una protección total. Se enmarca como el Segundo Servicio Crítico debido a la relevancia de mantener a la Institución libre de algún tipo de endeudamiento que pueda traerle problemas de carácter legal.

- **Servicio de Mantenimiento y Reparaciones**, se debe integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso. Pero también se añade el control de la infraestructura del edificio de la institución y el servicio de transporte. El administrador del Servicio deberá ser un profesional altamente capacitado en el manejo de servidores y todos aquellos implementos necesarios en el ámbito de la Tecnología de la Información. Además, deberá tener el acceso de personal cualificado para el cuidado y control de la infraestructura de la Institución, así como también aquellas personas conocedoras del manejo del servicio de transporte, cuidando que los señores conductores cuenten con la documentación adecuada para proveer el servicio, cuya información deberá reposar en los archivos del Servicio. Por lo expuesto es el Tercer Servicio Crítico de la Institución ya que su daño en el ámbito IT, Infraestructura o transporte paralizaría marcadamente a la Institución en lo expuesto, aunque su alteración no necesariamente detendría la misión de dar una educación integral, razón base del lugar que ocupa en este análisis.
- **Servicio Académico**, debe contar con información apropiada para la administración del ámbito académico con el fin de operar la entidad y para ejercer sus responsabilidades al dar clases y de cumplimiento. El administrador deberá tener acceso inmediato ante el requerimiento de los docentes de cualquier necesidad de repasar el PCI, PUD o cualquier otro documento para mejorar su eficiencia educativa. La mayoría de los archivos expuestos en el presente servicio se exponen en formato impreso, son susceptibles de ser consumidos por un incendio o fácilmente extraídos sin autorización. Es por eso considerarlo como Servicio Crítico, y ubicarlo en la cuarta posición de referencia.
- **Servicio de Gestión Humana**, está enfocado en mantener un medio ambiente adecuado para el personal de la Institución, a ello se añade el valor en apoyo que puede dar la Norma ISO 9004 en complemento con lo que señala el COBIT al mencionar: “*Cumplimiento*, se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto”. El administrador deberá

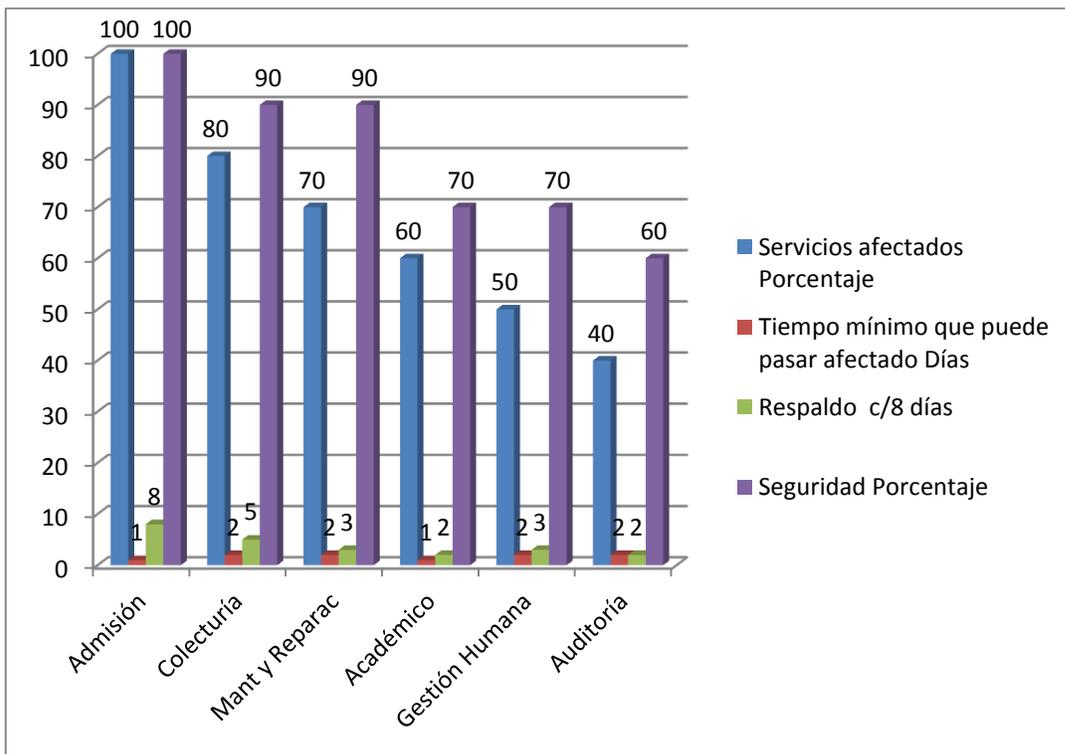
conocer perfectamente la norma ISO mencionada entre otras, así mismo las leyes, regulaciones y acuerdos contractuales, por lo que deberá estar altamente entrenado en el manejo de Internet para acceso a aquellas regulaciones mencionadas. Dominar el manejo de buscadores para acceso a aquellos programas que le permitan crear el ambiente para un mejor desenvolvimiento del personal, y facilitar las herramientas de trabajo que podrían ser requeridas por los miembros del Servicio, manteniendo una eficacia y eficiencia que le es propia a Gestión Humana. Los docentes y demás personal son parte fundamental del cumplimiento de la misión, de allí el valor crítico como Servicio.

- **Servicio de Auditoría**, permite establecer un resumen ejecutivo, marco referencial, objetivos de control, guías de auditoría, herramientas de implementación y guías de administración. El administrador deberá ser un profesional, conocer del campo de la auditoría, y básicamente de aquello referente a la Auditoría Informática, ya que será quien organice, direcciona y controle el buen desenvolvimiento de la IT en los diferentes Servicios. Por ello deberá estar claramente identificado con la norma ISO 27002, particularmente con lo expuesto en el numeral 10, referente a Gestión de Continuidad del Negocio, ya que estará en obligación permanente de comparar si lo que se realiza va acorde con lo expuesto en la norma citada. De allí porque se coloca al Servicio de Auditoría como el último servicio crítico de la Institución, ya que de él depende que los servicios anteriores vayan acorde a lo establecido y acordado entre los diferentes miembros de la Institución.

Respaldo según la necesidad de cada servicio.-

Servicios de la Institución	Servicios afectados	Tiempo mínimo que puede pasar afectado	Respaldo	Seguridad
	Porcentaje	Días	c/8 días	Porcentaje
<i>Admisión</i>	100	1	8	100
<i>Colecturía</i>	80	2	5	90
<i>Mant y Reparac</i>	70	2	3	90
<i>Académico</i>	60	1	2	70
<i>Gestión Humana</i>	50	2	3	70
<i>Auditoría</i>	40	2	2	60

Gráfico del respaldo según la necesidad de cada servicio.-



4. Desarrollo e Implementación del PCN.

Una vez que se ha definido la prioridad de los servicios críticos de la Institución, se realizará un análisis individual de cada uno de ellos para identificar los riesgos en cada servicio, análisis del impacto en el negocio (BIA): documentar el impacto (económico, reputación, pérdida de información, etc.) de la discontinuidad de los diferentes procesos de negocio, determinando:

- Período máximo de tiempo que los Servicios pueden encontrarse inoperativos.
- Nivel mínimo que los procesos deben alcanzar para ser operativos.
- Relaciones e interdependencias de los Servicios y recursos.

Identificar y evaluar las potenciales amenazas que podrían causar interrupciones. A partir de estos análisis, se identificarán las actividades críticas de la organización: actividades que tengan un impacto más grande en un periodo de tiempo más corto y que, por las necesidades del negocio, deben ser recuperadas rápidamente en caso de interrupción.

Para lo expuesto, serán analizados cada unos de los Servicios que conforman la Obra Educativa en un contexto individualizado, pero sin perder de vista la importancia de su interrelación con los otros Servicios, pero manteniendo el orden prioritario analizado en el capítulo II.

En un contexto general, el PCN en base al trabajo con los administradores y a las indagaciones realizadas se han encontrado los siguientes riesgos generales los cuales se refieren a desastres medio ambientales, disrupción organizada y deliberada, pérdida de los servicios y las utilidades y por servicio los cuales se refieren a crimen cibernético, pérdida de registros o datos, revelación de información sensible y fallos en los sistemas IT:

Se manejará la siguiente escala de valores:

PROBABILIDAD	
PUNTUACIÓN	NIVEL
1	MUY ALTO
2	ALTO
3	MEDIO
4	BAJO
5	MUY BAJO

4.1. RIESGOS GENERALES

RIESGO	CAUSAS	PROBABILIDAD	IMPACTO	BIENES EN RIESGO
Incendio Tormentas eléctricas Contaminación y amenazas medio ambientales.	Corte de energía eléctrica sin previo aviso. Instalaciones eléctricas defectuosas. Alambres sueltos sobre superficies susceptibles al fuego.	2	Perdida de datos e información sensible. Daños en los dispositivos electrónicos. Perdida de comunicación entre los servicios.	Equipo electrónico como: computador, impresora, regulador de voltaje, máquinas de escribir. Mueble de madera para guardar información relevante. Papeles de la institución con información sensible. Archivadores metálicos
Actos de sabotaje Robo	Manejo adecuado de ingeniería social para obtener información relevante. Obtención de dispositivos electrónicos sin autorización.	3	Obtención de información privilegiada. Perdida de dispositivos periféricos con información relevante.	Perdida de periféricos u otros dispositivos electrónicos de fácil acceso como ratones, reguladores u otros.

CONSECUENCIAS	< 2 horas	2 – 24 horas	24 – 48 horas	2 – 5 días	> 5 días
Impacto en el servicio al cliente por incendio	X				
Impacto en el servicio al cliente por tormentas eléctricas		X			
Impacto en el servicio al cliente por contaminación ambiental					X
Pérdida de clientes					X
Pérdida de ingresos			X		
Costos adicionales de recuperación potenciales		X			
Exposición a cláusulas penales					X
Exposición a posibles litigios					X

Pérdida de información clave	X				
Impacto financiero negativo		X			

4.2. RIESGOS POR SERVICIO

4.2.1. Riesgos del Servicio de Admisión.

RIESGO	CAUSAS	PROBABILIDAD	IMPACTO	BIENES EN RIESGO
Crimen Cibernético	Dispositivos portátiles	5	Demora en la entrega de reportes. Reportes mal elaborados.	Aplicaciones de Office 2007 Programa de base de Visual Fox Pro para generación de reportes mensuales: Sistema de Notas Archivos de información del personal docente de la institución. McAfee Anti – virus
Actos de sabotaje	Falsificación de notas Obtención de exámenes	4	Entrega de valores falsos al Ministerio de Educación	Perdida de periféricos u otros dispositivos electrónicos de fácil acceso como ratones, reguladores u otros. Archivos con información relevante sobre notas u otros.
Fallos en el sistema de comunicación	Mala conducción de electricidad. Matriz de comunicaciones mal empleada.	3	Estudiantes y padres de familia mal informados. Preocupación académica por información mal entregada.	Matriz de comunicación en archivos en el computador. Teléfonos y otros dispositivos de comunicación.
Fallos en el sistema de electricidad	Mal servicio eléctrico proporcionado por la empresa eléctrica.	3	Perdida de datos e información sensible. Daños en los dispositivos electrónicos. Daños en muebles de madera o similares.	Equipo electrónico como: regulador de voltaje, máquinas de escribir. Mueble de madera para guardar información relevante. Bodega de madera en segundo nivel con

				información en papel de la institución. Archivadores metálicos
--	--	--	--	---

4.2.1.1. Consecuencias del Servicio

CONSECUENCIAS	< 2 horas	2 – 24 horas	24 – 48 horas	2 – 5 días	> 5 días
Impacto en el servicio al cliente	X				
Pérdida de clientes				X	
Pérdida de ingresos				X	
Costos adicionales de recuperación potenciales			X		
Exposición a cláusulas penales					X
Exposición a posibles litigios					X
Pérdida de información clave	X				
Impacto financiero negativo		X			

4.2.2. Riesgos del Servicio de Colecturía.

RIESGO	CAUSAS	PROBABILIDAD	IMPACTO	BIENES EN RIESGO
Fallos en el sistema de electricidad.	Perdidas y bajones de electricidad por malas instalaciones eléctricas, además del consumo eléctrico de la empresa	5	Pérdida de la información contable	Equipo electrónico como: computadores, impresora, regulador de voltaje, UPS, máquinas de escribir. Mueble de madera para guardar información relevante. Bodega de madera en segundo nivel con material didáctico y suministros de oficina Archivadores metálicos
Robo	Padres de familia inescrupulosos y	5	Pérdida de archivos y datos contables.	Dispositivos periféricos de respaldo

	proveedores de servicio para la institución.			como discos duros externos u otros como pen – drives.
Fallos en el sistema de comunicación	Mala conducción eléctrica	4	Contabilidad deficiente carente de ciertos términos económicos	Programas de contabilidad, particularmente T – Max y Olimpo V7.

4.2.2.1. Consecuencias del Servicio

CONSECUENCIAS	< 2 horas	2 – 24 horas	24 – 48 horas	2 – 5 días	> 5 días
Impacto en el servicio al cliente	X				
Pérdida de clientes			X		
Pérdida de ingresos			X		
Costos adicionales de recuperación potenciales		X			
Exposición a cláusulas penales				X	
Exposición a posibles litigios			X		
Pérdida de información clave	X				
Impacto financiero negativo	X				

4.2.3. Riesgos del Servicio de Mantenimiento y Reparaciones.

RIESGO	CAUSAS	PROBABILIDAD	IMPACTO	BIENES EN RIESGO
Crimen Cibernetico	Básicamente Internet por el alto uso que se da dentro del Servicio.	5	Pérdida de la información mantenida en el Servidor principal de la Institución. Alumnos, alumnas sin material de trabajo.	Daños sobre el Servidor HP Proliant ML 150G6. Estaciones de trabajo (24 en total) Impresoras
Fallos en el sistema de electricidad.	Malas conexiones eléctricas. Amontonamiento de cables en un solo sitio.	4	Estrés permanente por la falta de protección. Alumnos, alumnas con una idea errada acerca de las instalaciones eléctricas.	Servidor Estaciones de trabajo DSL Wireless HUAWEI Echolife HG520s Switch 3COM Super Stack 3 3C16471 UPS APC

Actos de sabotaje.	Estudiantes sin valores morales o bromas carentes de sentido	3	Pérdida de archivos necesarios para el manejo del Sistema operativo Pérdida de periféricos	Estación de trabajo. Periféricos de tamaño pequeño como ratones, parlantes u otros.
--------------------	--	---	---	---

4.2.3.1. Consecuencias del Servicio

CONSECUENCIAS	< 2 horas	2 – 24 horas	24 – 48 horas	2 – 5 días	> 5 días
Impacto en el servicio al cliente		X			
Pérdida de clientes					X
Pérdida de ingresos				X	
Costos adicionales de recuperación potenciales			X		
Exposición a cláusulas penales					X
Exposición a posibles litigios					X
Pérdida de información clave			X		
Impacto financiero negativo	X				

4.2.4. Riesgos del Servicio Académico.

RIESGO	CAUSAS	PROBABILIDAD	IMPACTO	BIENES EN RIESGO
Crimen Cibernético	Dispositivos portátiles. No se actualiza el anti – virus.	5	Retraso en el orden cronológico para impartir la cátedra a través de los planes semanales.	Computadora personal Daños sobre los archivos que contienen los PCI, PUD, PEI.
Pérdida de registros o datos.	Información impresa que puede ser tomada por cualquier docente, administrativo o público en general con acceso al Servicio	3	Retraso en la entrega de calificaciones por pérdida de los cuadernos de control. Alteración en el proceso propio del Servicio.	Cuadernos de calificaciones y otros documentos de importancia de la institución.

4.2.4.1. Consecuencias del Servicio

CONSECUENCIAS	< 2 horas	2 – 24 horas	24 – 48 horas	2 – 5 días	> 5 días
Impacto en el servicio al cliente		X			
Pérdida de clientes					X
Pérdida de ingresos					X
Costos adicionales de recuperación potenciales			X		
Exposición a cláusulas penales					X
Exposición a posibles litigios					X
Pérdida de información clave		X			
Impacto financiero negativo		X			

4.2.5. Riesgos del Servicio de Gestión Humana.

RIESGO	CAUSAS	PROBABILIDAD	IMPACTO	BIENES EN RIESGO
Crimen Cibernético	Internet Dispositivos portátiles Empleados mal capacitados.	5	No existe intercambio de información ya que existe conflicto en la red propia del Servicio. La información sensible no permanece únicamente en el servicio.	Computadores personales (3 en total). Particularmente la computadora que se utiliza como Servidor para el control de dominios.
Actos de sabotaje.	Uso de ingeniería social para obtener la información a través de personal no entrenado.	4	Obtención de servicios personales. Impide el trabajo adecuado del servicio.	Archivos con información exclusiva. Impresión de archivos que no corresponden a las necesidades del departamento.
Robo	Sustracción de implementos electrónicos.	4	Pérdida de periféricos y otros dispositivos pequeños.	Ratones, parlantes y otros periféricos pequeños, incluidos pen-drives.
Revelación de información sensible.	Aplicación de ingeniería social.	4	Pérdida de credibilidad del personal.	Prestigio del Servicio de Gestión Humana.
Fallos en el sistema de electricidad	Mal servicio proporcionado por la empresa.	3	Daños en los dispositivos electrónicos.	Equipo electrónico como: computador personal como servi-

				<p>dor más 2 estaciones de trabajo, cada una de las cuales con su respectivo regulador de voltaje. Impresora Samsung ML – 2010. Scanner Ben-Q, impresora EPSON LX – 300. Router D – Link Dir – 300.</p> <p>Cada escritorio con su respectiva computadora descansa sobre una alfombra única para todos.</p> <p>Paredes de madera</p> <p>Mueble de madera para archivo de elementos propios del servicio.</p> <p>Archivadores metálicos.</p>
--	--	--	--	--

4.2.5.1. Consecuencias del Servicio

CONSECUENCIAS	< 2 horas	2 – 24 horas	24 – 48 horas	2 – 5 días	> 5 días
Impacto en el servicio al cliente		X			
Pérdida de clientes			X		
Pérdida de ingresos				X	
Costos adicionales de recuperación potenciales		X			
Exposición a cláusulas penales			X		
Exposición a posibles litigios				X	
Pérdida de información clave	X				
Impacto financiero negativo	X				

4.2.6. Riesgos del Servicio de Auditoría.

RIESGO	CAUSAS	PROBABILIDAD	IMPACTO	BIENES EN RIESGO
Revelación de información sensible.	Ingeniería social. Personal mal capacitado.	5	Las normas de la Institución no van acorde con las establecidas en la Norma ISO.	Archivos del Servicio contenido en Office 2007 particularmente Excel.
Actos de sabotaje.	Uso de ingeniería social para obtener la información a través de personal no entrenado.	4	Se altera la información base y el personal no se compromete con el trabajo.	Registros y datos de seguimiento acorde con la Norma ISO.
Crimen Cibernetico.	Dispositivos periféricos.	4	Daños en el Sistema Operativo. Pérdida de archivos, registros y datos.	Servidor DELL Power Edge SC 440 Backups – UPS RS 1200 APC Impresora HP Laser P2015 dn Kypus Server Appliance. Router EDIMAX EW 7209 APg. Estaciones de trabajo Vía Samuel 2 (10 en total)

4.2.6.1. Consecuencias del Servicio

CONSECUENCIAS	< 2 horas	2 – 24 horas	24 – 48 horas	2 – 5 días	> 5 días
Impacto en el servicio al cliente		X			
Pérdida de clientes			X		
Pérdida de ingresos				X	
Costos adicionales de recuperación potenciales			X		
Exposición a cláusulas penales			X		
Exposición a posibles litigios				X	
Pérdida de información clave		X			
Impacto financiero negativo	X				

5. Seguridades a los Servicios Críticos.

A continuación realizaremos una definición explícita de los causales físicos y lógico de daño a cada Servicio en estudio, así mismo, se revisará como se ejecuta la recuperación del desastre, la recuperación de la Institución y como se terminará de restaurar por completo las funciones de los servicios afectados.

“Los tres principios fundamentales de la gestión de seguridad, a saber, confidencialidad, integridad y disponibilidad, denominados a menudo la triada Confidencialidad, Integridad, Disponibilidad (CID), tienen como objetivo implantar los mecanismos necesarios para salvaguardar la información frente a todo tipo de ataques y amenazas”⁵

5.1. Seguridades Generales a los Servicios Críticos

RIESGO	CAUSAS	CONSECUENCIA	SOLUCIÓN
Incendio Tormentas eléctricas Contaminación y amenazas medio ambientales.	Corte de energía eléctrica sin previo aviso. Instalaciones eléctricas defectuosas. Alambres sueltos sobre superficies susceptibles al fuego.	Daños en los computadores de escritorio, estaciones de trabajo, servidores, y demás implementos electrónicos. Daños en los materiales de madera como muebles, escritorios y archivadores.	Utilización de extintores tipo ABC. Utilización de UPS para resguardar la información Verificación de la conducción eléctrica de los conectores manteniendo el nivel de ohm requeridos.
Actos de sabotaje Robo	Manejo adecuado de ingeniería social para obtener información relevante. Obtención de dispositivos electrónicos sin autorización.	Alteración de contraseñas para manipular información relevante. Pérdida de periféricos	Uso de contraseñas que incluya el uso de letras, números y símbolos. Bitácoras de seguimiento de los implementos y obligación de firmar el uso del implemento.

* Quizá sería de utilidad la instalación de una planta eléctrica propia, pero cuyo costo rebasa las posibilidades económicas de la Institución, sin embargo su probable uso está en estudio en el colegio.

⁵ ALVAREZ, G., PEREZ, P. (2004): Seguridad Informática para empresas y particulares. Madrid: Ed. McGraw Hill.

5.2. Seguridades por Servicio

5.2.1. Servicio de Admisión

RIESGO	CAUSAS	CONSECUENCIA	SOLUCIÓN
Crimen Cibernético	Dispositivos portátiles	Pérdida de la información	Actualización permanente del anti – virus. IDS Sistema Detector de Intrusos, particularmente el programa SNORT que constituye un GNU libre. Firewall, particularmente Ad – Aware cuyo uso gratuito es muy útil.
Actos de sabotaje	Falsificación de notas Obtención de exámenes	Promoción de un alumno no apto para cursar un nivel superior.	Uso de contraseñas que incluya el uso de letras, números y símbolos. Steganos Password Manager (SPM) para encriptar las contraseñas y mantenerlos en un solo sitio físico
Fallos en el sistema de comunicación	Mala conducción de electricidad. Matriz de comunicaciones mal empleada.	Reportes mal elaborados. Retraso en la entrega de documentos de soporte.	Matriz de comunicaciones basada en gráficas de reconocimiento para cada uno de los empleados. Uso de alimentadores continuos de energía.
Fallos en el sistema de electricidad	Mal servicio eléctrico proporcionado por la empresa eléctrica.	Apagones sin previo aviso que produce la pérdida de información importante.	UPS que permite la mantención de la información un tiempo prudente para poder ser salvadas con éxito. Respaldo de la información permanente al término de la jornada de trabajo.

5.2.2. Servicio de Colecturía

RIESGO	CAUSAS	CONSECUENCIA	SOLUCIÓN
Fallos en el sistema de electricidad.	Perdidas y bajas de electricidad por malas instalaciones eléctricas, además del consumo mal servicio eléctrico de la empresa	Daños en los equipos tecnológicos.	Alimentador continuo de energía como UPS para salvaguardar la última información utilizada. Revisión de posibles cortes eléctricos para prevenir el fallo.
Robo	Padres de familia inescrupulosos y proveedores de	Pérdida de hardware y material tecnológico para	Atención exclusiva a través de ventanilla para impedir el acceso a la oficina principal.

	servicio para la institución.	el manejo de la información.	Uso de contraseñas que incluya el uso de letras, números y símbolos. Steganos Password Manager para encriptar las contraseñas y mantenerlos en el mismo sitio físico del Servicio de Admisión.
Fallos en el sistema de comunicación	Mala conducción eléctrica	Entrega de reportes de pagos de matrícula y sueldos deficientes	Pedir la revisión continua por parte del Consejo Nacional de Telecomunicaciones (CNT) para mejorar la conducción eléctrica.

5.2.3. Servicio de Mantenimiento y Reparaciones

RIESGO	CAUSAS	CONSECUENCIA	SOLUCIÓN
Crimen Cibernético	Básicamente Internet por el alto uso que se da dentro del Servicio.	Pérdida de información. Servicio de Internet en extremo lento.	Preferencia del uso del Sistema Operativo Linux para administración de la red. IDS como Snort que es un GNU libre Kerios como medio de control de los dominios a través de Windows Server 2003. Nmap – Zenmap GUI como lo señala textualmente: “Nmap is a free and open source utility for network operation and security auditing”. Que permitirá el control de todos los dispositivos de red conectado al Servidor Central ubicado en este Servicio.
Fallos en el sistema de electricidad.	Malas conexiones eléctricas. Amontonamiento de cables en un solo sitio.	Peligro de incendio. Apagado imprevisto de las computadoras.	Mantener un extintor de incendio tipo ABC actualizado. Proveer de una unidad eléctrica para conexión que permita mantener en orden los cables expuestos. Recubrimiento plástico de los cables para formar un solo conjunto.
Actos de sabotaje.	Estudiantes sin valores morales o bromas carentes de sentido	Daños en el sistema operativo y archivos específicos.	Enfatizar el valor de la honestidad, respeto y don de servicio para con nuestros congéneres.

5.2.4. Servicio Académico

RIESGO	CAUSAS	CONSECUENCIA	SOLUCIÓN
Crimen Cibernético	Dispositivos portátiles. No se actualiza el anti – virus.	Pérdida de información referente a los planes de los docentes.	Actualización permanente del anti – virus. IDS Snort Firewall Ad – aware Actualización permanente del sistema operativo.
Pérdida de registros o datos.	Información impresa que puede ser tomada por cualquier docente, administrativo o público en general con acceso al Servicio	Sustracción de cuadernos de calificaciones y documentos impresos importantes.	Limitar el acceso del personal. Atención al público en otras instancias de la Institución. Mantener bajo llave todo documento referente al docente particularmente.

5.2.5. Servicio de Gestión Humana

RIESGO	CAUSAS	CONSECUENCIA	SOLUCIÓN
Crimen Cibernético	Dispositivos portátiles.	Conflicto de red. Aterrizaje de disco duro. Pérdida de información.	Anti – virus actualizado. IDS como Snort que es un GNU libre Kerios como medio de control de los dominios a través de Windows Server 2003. Nmap – Zenmap GUI como lo señala textualmente: “Nmap is a free and open source utility for network operation and security auditing”. Que permitirá el control de todos los dispositivos de red conectado al Servidor Central ubicado en este Servicio. Mejor capacitación al personal del Servicio.
Actos de sabotaje.	Uso de ingeniería social para obtener la información a través de personal no entrenado.	Chantaje. Cambios de contraseña originales.	Limitar el número de personas que ingresan. Control de las personas que son atendidas. Steganos Password Manager para encriptar las contraseñas y mantenerlos en el mismo sitio físico del Servicio de Admisión.

Robo	Sustracción de implementos electrónicos.	No se puede utilizar adecuadamente los implementos.	Limitar el número de personas que ingresan. Control de las personas que son atendidas. Control de los implementos pertenecientes al Servicio utilizando un código propio.
Revelación de información sensible.	Aplicación de ingeniería social.	Conocimiento de información de utilidad exclusiva del Servicio.	Entrenar al personal para que conozca cuáles son las limitaciones y disponibilidad de información que puede ser o no entregada.
Fallos en el sistema de electricidad	Mal servicio proporcionado por la empresa.	Daños al sistema operativo y equipo electrónico en general.	UPS que permite la mantención de la información un tiempo prudente para poder ser salvadas con éxito. Respaldo de la información permanente al término de la jornada de trabajo.

5.2.6. Servicio de Auditoría

RIESGO	CAUSAS	CONSECUENCIA	SOLUCIÓN
Revelación de información sensible.	Ingeniería social. Personal mal capacitado.	Mala comparativa entre normas.	Seleccionar mejor personal de auditoría.
Actos de sabotaje.	Uso de ingeniería social para obtener la información a través de personal no entrenado.	Se altera la información base y el personal no se compromete con el trabajo.	Impedir entregar información sensible a personal no autorizado. Mantener un entrenamiento permanente para un adecuado servicio de auditoría dentro de la institución.
Crimen Cibernético.	Dispositivos periféricos.	Daño eminente a la información relevante.	Mejorar la calidad de los anti – virus.

Otros aspectos relevantes a la protección de los servicios y demás implementos de la Institución se detallan en el capítulo 8 del presente proyecto, allí se incluyen detalles referentes a:

- Estrategias de backups y recuperación de los sistemas IT.
- Cobertura de seguro
- Proveedores y personal clave del PCN
- Organigrama funcional
- Equipo de recuperación del desastre
- Documentación y registros vitales de procesos de la Institución
- Almacenamiento fuera de la Institución
- Procedimientos para el manejo de padres de familia, proveedores y público en general
- Autorización para la protección en caso de emergencia.

6. Sistema de Comunicaciones

Es de particular importancia al momento de evaluar los riesgos de la institución y el impacto de las emergencias potenciales, considerar la interrupción y disponibilidad de los servicios de IT y comunicaciones. El nivel de dependencia que tiene la Obra Educativa, como lo señalamos en párrafos anteriores, de los sistemas de IT y las comunicaciones y la naturaleza de los servicios al cliente que suelen estar disponibles 7x24, esto es particularmente notorio en el servicio WEB que brinda la Institución, significa que es esencial que las organizaciones mantengan operativas sus redes de IT y los sistemas de comunicación operacionales todo el tiempo. Esta sección examina algunos de los temas a considerar cuando se evalúa el riesgo asociado con los servicios IT y las comunicaciones.

Por otro lado, el sistema de comunicación en la Institución se maneja en la siguiente manera: en el Servicio de Mantenimiento y Reparación se conserva el servidor principal, esto es el Servidor HP Proliant ML 150G6, quién constituye el eje de la red, a través del switch 3COM Super Stack 3 3C16471 se comunica directamente con el resto de servicios, esto es Admisión, Colecturía, Académico, Gestión Humana. Es decir la topología básica del servicio es en estrella.

Sin embargo, el Servicio de Gestión Humana también tiene su servidor principal a través de una computadora de usuario básica, quién controla el resto de implementos tecnológicos y genera un punto de acceso a través del router d – link dir 300, para acceso a los otros servicios de la Institución.

El Servicio de Auditoría, por disposición de la Curia Diocesana mantiene un servidor individualizado tipo DELL Power Edge SC 440, la cual se conecta a un conjunto de 10 estaciones de trabajo que son de utilidad para el personal de la Institución básicamente, pero también son de utilidad para los y las estudiantes a través de un Kypus Server Appliance. Esto permite que este Servicio mantenga básicamente uno de sus principios básicos, el Principio de Independencia: “obliga al auditor a exigir una total autonomía e independencia en su trabajo, condición ésta imprescindible para permitirle actuar libremente según sea su leal saber y entender”⁶

6.1. Especificaciones, sistemas de comunicación y dependencias de la Institución

El PCN debe contener una especificación detallada de los principales sistemas de procesamiento IT del negocio y las configuraciones de las redes. Esta lista debe contener los procesos de la Obra claves que dependen de cada componente del sistema. También es importante que los documentos de especificaciones se actualicen cada vez que los sistemas de IT cambien. Conforme

⁶ PIATTINI, M., DEL PESO, E. (2001): Auditoría Informática, un enfoque práctico. México D.F.: Ed. Alfaomega – RAMA.

el Servicio de la institución, utilizaremos una matriz que nos dé una idea clara de los componentes en hardware y software que mantiene el Servicio, para una idea clara ver el Anexo 4.

El equipo del PCN se ubica en:

SERVICIO	RESPONSABLE OFICIAL	NOMBRE	UBICACIÓN
Admisión	ADP (administrador del proceso) Colaborador	Lic. Ana Cobos Srta. Carolina Yamberla	Oficina de Inspección, departamento de Secretaría, segundo piso, Edificio Fray Saturnino Gutiérrez.
Colecturía	ADP Colaborador	Lic. Norma Lincango Srta. Ana Pacheco	Departamento de Colecturía, primer piso, Edificio Fray Saturnino Gutiérrez, lado derecho de la puerta de ingreso principal.
Mantenimiento y Reparaciones	ADP Colaborador	Lic. José Luis Rodríguez MSc. Juan Carlos Cobos	Laboratorio de Computación, sección bachillerato, Edificio Fray Saturnino Gutiérrez. Segundo piso.
Académico	ADP Colaborador	Lic. Guadalupe Tituaña Lic. Viviana Abata	Oficina de Inspección, departamento del Vice – rectorado, segundo piso, Edificio Fray Saturnino Gutiérrez junto al Rectorado.
Gestión Humana	ADP Colaborador	Lic. Yolanda Yanez Ing. Patricio Martínez	Departamento de Orientación y Bienestar Estudiantil, Departamento de Gestión Humana, Tercer Piso. Edificio Fray Saturnino Gutiérrez.
Auditoría	ADP Colaborador	Lic. Pedro Auz Lic. Mariana Colahuazo	Laboratorio de Contabilidad, Edificio Fray Saturnino Gutiérrez a la izquierda de las gradas al acceso principal. Segundo piso.

6.2. Personal Clave

Vamos a realizar una matriz para información sobre cada una de las personas claves responsables por la ejecución de los procedimientos de emergencia. Estas personas deben estar familiarizadas con la implementación de estos procedimientos y deben recibir toda la capacitación necesaria para desarrollar dichas tareas específicas o técnicas.

SERVICIO	RESPONSABLE OFICIAL	NOMBRE	PERSONAL BACKUPS	CONTACTO	CONTACTO DE EMERGENCIA
Admisión	ADP (administrador del proceso)	Lic. Ana Cobos	MSc. Juan Carlos Cobos	2956921	n/a
	Colaborador	Srta. Carolina Yamberla		3450811	n/a
Colecturía	ADP	Lic. Norma Lincango	MSc. Juan Carlos Cobos	2037616	095626729
	Colaborador	Srta. Ana Pacheco		n/a	093777201
Mantenimiento y Reparaciones	ADP	Lic. José Luis Rodríguez	MSc. Juan Carlos Cobos	n/a	097445418
	Colaborador	MSc. Juan Carlos Cobos		2433945	097859064
Académico	ADP	Lic. Guadalupe Tituaña	MSc. Juan Carlos Cobos	3432759	087476551
	Colaborador	Lic. Viviana Abata		n/a	095221533
Gestión Humana	ADP	Lic. Yolanda Yanez	Ing. Patricio Martínez	3130243	n/a
	Colaborador	Ing. Patricio Martínez		2351464	096296102
Auditoría	ADP	Lic. Pedro Auz	Curia Diocesana	2486217	n/a
	Colaborador	Lic. Mariana Collahuazo		2842915	n/a

6.3. Servicios externos de emergencia

El PCN debe contener información sobre los servicios públicos de emergencia y otros proveedores de servicios de emergencia privados y es evidente que dentro de la Institución su necesidad es imperiosa, así a través de otra matriz demostramos cuáles son esos servicios y acotamos su forma de contacto:

SERVICIO	NÚMERO DE CONTACTO	NOMBRE DEL CONTACTO
Bomberos	911/122; 2245674	Luis Hernán Correa, Estación #5, Sector Jipijapa.
Ambulancia	911	Médico de turno
Policía	2450648/095432973	Oficial de turno, Estación Río Coca, Sector Jipijapa.
Servicio de Seguridad	099257730	Capitán (retirado) Wilmer Arze Ocaña Guerra

7. Planes del PCN

Al preparar el PCN es necesario considerar si es adecuado contar con una amplia gama de procedimientos de recuperación de desastres. Este capítulo revisa procedimientos de recuperación para un mejor desenvolvimiento dentro de la Continuidad del Negocio.

Además, se debe definir que el PCN contiene dos planes añadidos: Plan de Recuperación del Desastre y el Plan de Recuperación del Negocio. El primero de ellos es aquel elemento que contribuye a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operatividad mínima luego de una contingencia, en la que se vean afectados los Servicio y recursos informáticos que sostiene la Institución.

El segundo, es decir, el Plan de Recuperación del Negocio, implica la restauración de las operaciones normales de la Institución luego de un evento inesperado que interrumpió todos o parte de los Servicios. Desde la perspectiva de la Institución, esta es la fase más crítica de todo el PCN. La eficiencia y eficacia de los procedimientos que forman parte de esta sección pueden tener una incidencia directa en la habilidad de la organización para sobrevivir. Cada uno de estos es ampliamente explicado a lo largo del presente capítulo, así también se verán definidos los miembros de cada plan estudiado.

7.1. Plan de Recuperación del Negocio

7.1.1. Autoridades en el mantenimiento del edificio

Esta sección del PCN contiene una lista de todos los Servicios de la Institución y la información acerca de cada una en relación a:

7.1.1.1. *Instalaciones Propias.*

Para el ámbito de los implementos informáticos de acuerdo al Servicio que provee estás reúnen las siguientes características:

En el **Servicio de Admisión** el responsable del mantenimiento es el MSc. Juan Carlos Cobos, la responsabilidad ante una emergencia se maneja a través del siguiente proceso:

Aprobaciones externas necesarias antes de comenzar las tareas: Sor Zoila Pacheco, Rectora de la Institución

Aprobaciones internas necesarias antes de contactar a los contratistas: Lcda. Ana Cobos, Secretaria

Procedimientos para obtener las aprobaciones en situaciones de emergencia:

Identificación del estado de desastre potencial:

Una de las primeras tareas es determinar si la crisis actual o latente es lo suficientemente grave como para requerir la evacuación del personal. Todos los Servicios deben testear sus procedimientos de evacuación para maximizar la seguridad de los empleados. El servicio de Admisión cuenta con dos puertas de salidas una que recorre hacia el rectorado de la Institución y otra que le permite la salida inmediata al corredor principal de las oficinas del Servicio.

Si ocurrió una situación de emergencia grave, que causó heridas o muertes o el daño de las instalaciones o equipos, el Equipo de recuperación del desastre debe movilizarse de inmediato.

El criterio para determinar si una situación de potencial desastre existe puede contemplar lo siguiente:

- Si existe amenaza actual o potencial a la seguridad humana
- Si existe amenaza seria actual o potencial a los edificios o equipos
- Si hay alguna posibilidad de que sea necesario involucrar a los servicios de emergencia
- Si la respuesta a alguna de los interrogantes arriba mencionados es positiva, entonces se debe notificar al Equipo de recuperación del desastre.

Involucrar a los servicios de emergencia:

Los servicios de emergencia necesitan contactarse con individuos responsables de la organización que les provean la información requerida, estos servicios de emergencia están expuestos en el capítulo previo. Una vez que la situación de emergencia esté bajo control, los servicios de emergencia manejarán la situación con los oficiales representantes de la organización. Este suele ser el equipo de recuperación del desastre. En el servicio de admisión está encabezado por el Lcdo. José Luis Rodríguez y el Ing. Marco Bravo, como dueño del sistema de notas, así como el apoyo del MSc. Juan Carlos Cobos. Este equipo además proveerá asistencia en el terreno si se requiere otro tipo de especialistas.

Evaluar el impacto potencial de la emergencia en el negocio:

El Servicio de Admisión, al igual que el otro conjunto de Servicios en estudio, hará evaluaciones durante varias de las etapas del proceso de recuperación dependiendo de la escala de la emergencia desde la perspectiva del negocio. Durante el proceso de recuperación del desastre, se incluirá una evaluación preliminar del daño. El Equipo de recuperación del desastre llevará a cabo las evaluaciones iniciales.

Las evaluaciones están basadas en las circunstancias particulares y consideraremos como escala apropiada, la siguiente:

EVENTO DISRUPTIVO CON IMPACTO POTENCIAL EN EL LARGO PLAZO

1	Es posible que afecte las operaciones normales de negocio por más de cuatro semanas
2	Es posible que afecte las operaciones normales de negocio entre una y cuatro semanas
3	Es posible que afecte las operaciones normales de negocio por más de una semana

Movilizar al equipo de recuperación del desastre:

Una de las tareas a realizar durante las etapas tempranas de la emergencia es notificar al DRT (Disaster Recovery Team) de la ocurrencia de la misma. La notificación solicitará a los miembros del DRT que se junten en el sitio del problema. Además involucrará la suficiente información como para que la solicitud sea comunicada de manera efectiva.

El Líder del Equipo (Ing. Patricio Martínez) del PCN será alertado inicialmente y, a su vez, será el responsable de notificar al resto del DRT quiénes asistirán al sitio de emergencia. En caso de que el líder no se encuentre o no se le haya podido notificar, su reemplazo será la Vicerrectora de la Institución, Lcda. Guadalupe Tituaña.

Esta sección del PCN contiene una lista de las personas a contactar como se evidencia en los párrafos previos y los que se emiten a continuación, pero a todos los Servicios se añadirá:

- La información de contacto,
- El tiempo y día del contacto,
- Quién realizó el contacto,
- A quién se le comunicó el mensaje,
- Las instrucciones a seguir,
- La respuesta,
- El tiempo en el que llegará al sitio.

Notificación a los gerentes y empleados clave:

Durante la fase de recuperación de desastre, los gerentes y empleados claves se mantendrán informados de los desarrollos claves que afecten al proceso general del negocio y que impacten en particular sobre sus áreas de responsabilidad. Si, la emergencia ocurre fuera de las horas de trabajo, será necesario instruir a los empleados para que se queden en sus hogares hasta que reciban otras instrucciones. Sin embargo si el Servicio de Admisión considera pertinente también que los empleados claves y ciertos miembros gerenciales pueden, por el otro lado, ser requeridos en el sitio de emergencia o el centro de comando desde los inicios del proceso para trabajar sobre cómo minimizar el impacto de la emergencia en las áreas de su responsabilidad deberán acudir a la Institución.

El Líder del equipo PCN o su reemplazo es responsable de llevar a cabo esta actividad.

Esta sección del PCN conoce que los empleados claves de esta sección son la Lcda. Ana Cobos y la Srta. Carolina Yamberla y el gerente principal se mantiene la Rectora Sor Zoila Pacheco. El listado del personal clave de este Servicio y el resto de servicios se detallan en el capítulo 6.

Notificación a los familiares:

Si la emergencia puede provocar la preocupación de los familiares de algún empleado, debido a la hospitalización del mismo, es necesario notificar a la familia directa inmediatamente. Este tipo de comunicación necesita manejarse con sensibilidad y cuidado de modo de no aumentar el nivel de estrés de las personas a las que se notifica. Este tipo de tarea está a cargo del ADP del Servicio de Gestión Humana Lcda. Yolanda Yáñez, esta parte del análisis se enfoca a todos los servicios en general. Si se requiere apoyo psicológico para dárselo a los familiares, se cuenta con la Dra. Gabriela Serrano y la Dra. Belén Rodríguez.

Manejo de la información a los padres de familia, proveedores y público en general:

El contacto con los padres de familia, proveedores y público en general durante la fase de recuperación del desastre debe manejarse cuidadosamente. Toda la información emitida al público en esta instancia debe ser apropiada y se debe reducir la especulación al mínimo. Las comunicaciones a padres, proveedores y público deben estar a cargo de personas específicamente autorizadas para llevar a cabo esas tareas, en el Servicio de Admisión Sor Zoila Pacheco, Lcda. Ana Cobos. Otras personas que no hayan sido autorizadas deben ser fuertemente desalentadas a hacerlo. La política establecida es la atención en la Sala de Entrevistas junto al vice - rectorado por adelantado, para que sea seguida por la persona autorizada al momento de emitir información para el público.

Registro de los eventos:

Es importante que se registren todos los eventos clave durante la fase de recuperación del desastre. El Equipo de Recuperación del Desastre (DRT) debe mantener un registro de los eventos. Este registro inicia al comienzo de la emergencia. El Equipo de Recuperación del Negocio (BRT) que se especifica más adelante, debe tener una copia de este registro una vez que los peligros iniciales fueron controlados.

El Servicio de Admisión al igual que los demás servicios lleva el siguiente registro de eventos:

REGISTRO DE EVENTOS	
FECHA:	
HORA:	
TÍTULO:	
DESCRIPCIÓN (Realizarlo en forma resumida):	
SEGUIMIENTO (En caso de ser requerido):	

Personal responsable de las actividades de recuperación de las instalaciones y los datos de contacto ante emergencias: Msc. Juan Carlos Cobos.

Personal responsable de aprobar las reparaciones o reemplazos de los equipos, muebles y los datos de contacto ante emergencias: Lcdo. José Luis Rodríguez

En el **Servicio de Colecturía** el responsable del mantenimiento es el MSc. Juan Carlos Cobos, la responsabilidad ante una emergencia se maneja a través del siguiente proceso:

Aprobaciones externas necesarias antes de comenzar las tareas: Sor Zoila Pacheco, rectora

Aprobaciones internas necesarias antes de contactar a los contratistas: Lcda. Norma Lincango

Procedimientos para obtener las aprobaciones en situaciones de emergencia:

Identificación del estado de desastre potencial:

Una de las primeras tareas es determinar si la crisis actual o latente es lo suficientemente grave como para requerir la evacuación del personal. El servicio de Colecturía cuenta con una sola puerta de salida pero que apunta directamente a la puerta principal de la Institución haciendo efectiva la etapa de evacuación. Los demás aspectos son los mismos enunciados en el Servicio de Admisión.

Involucrar a los servicios de emergencia:

En el Servicio de Colecturía está encabezado por la Lcda. Norma Lincango y el MSc Juan Carlos Cobos. Este equipo además proveerá asistencia en el terreno si se requiere otro tipo de especialistas.

Evaluar el impacto potencial de la emergencia en el negocio:

Lo expuesto en el Servicio de Admisión

Movilizar al equipo de recuperación del desastre:

Lo expuesto en el Servicio de Admisión

Notificación a los gerentes y empleados clave:

Esta sección del PCN conoce que los empleados claves de esta sección son la Lcda. Norma Lincango y la Srta. Ana Pacheco y el gerente principal se mantienen la Rectora Sor Zoila Pacheco. El listado del personal clave de este Servicio y el resto de servicios se detallan en el capítulo 6.

El registro de los eventos, el manejo de la información a los padres de familia, proveedores y público en general, así como la notificación a los familiares será manejado en idéntica forma como se describe en el Servicio de Admisión.

Personal responsable de las actividades de recuperación de las instalaciones y los datos de contacto ante emergencias: MSc Juan Carlos Cobos

Personal responsable de aprobar las reparaciones o reemplazos de los equipos, muebles y los datos de contacto ante emergencias: Lcdo. José Luis Rodríguez.

En el **Servicio de Mantenimiento y Reparaciones** el responsable del mantenimiento es el Lic. José Luis Rodríguez, la responsabilidad ante una emergencia se maneja a través del siguiente proceso:

Aprobaciones externas necesarias antes de comenzar las tareas: Sor Zoila Pacheco, rectora

Aprobaciones internas necesarias antes de contactar a los contratistas: Lcdo. José Luis Rodríguez, MSc. Juan Carlos Cobos

Procedimientos para obtener las aprobaciones en situaciones de emergencia:

Identificación del estado de desastre potencial:

Una de las primeras tareas es determinar si la crisis actual o latente es lo suficientemente grave como para requerir la evacuación del personal. El servicio de Mantenimiento y Reparaciones cuenta con una sola puerta de salida hacia el corredor del edificio central de la Institución “Fray Saturnino Gutiérrez”. Los demás aspectos son los mismos enunciados en el Servicio de Admisión.

Involucrar a los servicios de emergencia:

En el Servicio de Mantenimiento y Reparaciones está encabezado por el Lcdo. José Luis Rodríguez y el MSc Juan Carlos Cobos, además del apoyo de los licenciados: Patricio Andrade, Lcdo. Juan Carlos Jurado, Lcda. Amparo Buitron. Este equipo además proveerá asistencia en el terreno si se requiere otro tipo de especialistas.

Evaluar el impacto potencial de la emergencia en el negocio:

Lo expuesto en el Servicio de Admisión

Movilizar al equipo de recuperación del desastre:

Lo expuesto en el Servicio de Admisión

Notificación a los gerentes y empleados clave:

Esta sección del PCN conoce que los empleados claves de esta sección son el Lcdo. José Luis Rodríguez y el MSc. Juan Carlos Cobos y el gerente principal se mantiene la Rectora Sor Zoila Pacheco. El listado del personal clave de este Servicio y el resto de servicios se detallan en el capítulo 6.

El registro de los eventos, el manejo de la información a los padres de familia, proveedores y público en general, así como la notificación a los familiares será manejado en idéntica forma como se describe en el Servicio de Admisión.

Personal responsable de las actividades de recuperación de las instalaciones y los datos de contacto ante emergencias: MSc Juan Carlos Cobos.

Personal responsable de aprobar las reparaciones o reemplazos de los equipos, muebles y los datos de contacto ante emergencias: Lcdo. José Luis Rodríguez

En el **Servicio Académico** el responsable del mantenimiento es el MSc. Juan Carlos Cobos, la responsabilidad ante una emergencia se maneja a través del siguiente proceso:

Aprobaciones externas necesarias antes de comenzar las tareas: Sor Zoila Pacheco, rectora

Aprobaciones internas necesarias antes de contactar a los contratistas: Lcda. Guadalupe Tituaña.

Procedimientos para obtener las aprobaciones en situaciones de emergencia:

Identificación del estado de desastre potencial:

Una de las primeras tareas es determinar si la crisis actual o latente es lo suficientemente grave como para requerir la evacuación del personal. El servicio Académico cuenta con una salida hacia el pasillo principal de la Secretaría, además sus paredes son elaboradas en madera, de tal forma que su forzamiento puede volverse simple. Los demás aspectos son los mismos enunciados en el Servicio de Admisión.

Involucrar a los servicios de emergencia:

En el Servicio Académico está encabezado por la Lcda. Guadalupe Tituaña, su apoyo esta dado por el cuerpo del Servicio Académico donde se incluye las licenciadas: MSc. Rocío Toapaxi, Lcda. Carla Enríquez, Lcdo. Carlos Peña, Lcdo. Henry Abril, Lcda. Viviana Abata. Este equipo además proveerá asistencia en el terreno si se requiere otro tipo de especialistas.

Evaluar el impacto potencial de la emergencia en el negocio:

Lo expuesto en el Servicio de Admisión

Movilizar al equipo de recuperación del desastre:

Lo expuesto en el Servicio de Admisión

Notificación a los gerentes y empleados clave:

Esta sección del PCN conoce que los empleados claves de esta sección son la Lcda. Guadalupe Tituaña, el MSc. Juan Carlos Cobos y el gerente principal se mantiene la Rectora Sor Zoila Pacheco. El listado del personal clave de este Servicio y el resto de servicios se detallan en el capítulo 6.

El registro de los eventos, el manejo de la información a los padres de familia, proveedores y público en general, así como la notificación a los familiares será manejado en idéntica forma como se describe en el Servicio de Admisión.

Personal responsable de las actividades de recuperación de las instalaciones y los datos de contacto ante emergencias: MSc. Juan Carlos Cobos

Personal responsable de aprobar las reparaciones o reemplazos de los equipos, muebles y los datos de contacto ante emergencias: Lcdo. José Luis Rodríguez

En el **Servicio de Gestión Humana** el responsable del mantenimiento es el Ing. Patricio Martínez, la responsabilidad ante una emergencia se maneja a través del siguiente proceso:

Aprobaciones externas necesarias antes de comenzar las tareas: Sor Zoila Pacheco, rectora.

Aprobaciones internas necesarias antes de contactar a los contratistas: Lcda. Yolanda Yáñez e Ing. Patricio Martínez.

Procedimientos para obtener las aprobaciones en situaciones de emergencia:

Identificación del estado de desastre potencial:

Una de las primeras tareas es determinar si la crisis actual o latente es lo suficientemente grave como para requerir la evacuación del personal. El servicio de Gestión Humana cuenta con puertas individualizadas por cada departamento que forma parte del servicio. Los demás aspectos son los mismos enunciados en el Servicio de Admisión.

Involucrar a los servicios de emergencia:

En el Servicio de Gestión Humana está encabezado por la Lcda. Yolanda Yáñez y el Ing. Patricio Martínez. Este equipo además proveerá asistencia en el terreno si se requiere otro tipo de especialistas.

Evaluar el impacto potencial de la emergencia en el negocio:

Lo expuesto en el Servicio de Admisión

Movilizar al equipo de recuperación del desastre:

Lo expuesto en el Servicio de Admisión

Notificación a los gerentes y empleados clave:

Esta sección del PCN conoce que los empleados claves de esta sección son la Lcda. Yolanda Yáñez, el Ing. Patricio Martínez y el personal de apoyo incluido el personal del Servicio de Psicología, quienes son la Dra. Gabriela Serrano, Dra. Belén Rodríguez, Lcda. Doris Rea, Lcda. Cecilia Chiluisa y

el gerente principal se mantiene la Rectora Sor Zoila Pacheco. El listado del personal clave de este Servicio y el resto de servicios se detallan en el capítulo 6.

El registro de los eventos, el manejo de la información a los padres de familia, proveedores y público en general, así como la notificación a los familiares será manejado en idéntica forma como se describe en el Servicio de Admisión.

Personal responsable de las actividades de recuperación de las instalaciones y los datos de contacto ante emergencias: Ing. Patricio Martínez.

Personal responsable de aprobar las reparaciones o reemplazos de los equipos, muebles y los datos de contacto ante emergencias: Lcdo. José Luis Rodríguez.

En el **Servicio de Auditoría** el responsable del mantenimiento es el Lcdo. Pedro Auz, la responsabilidad ante una emergencia se maneja a través del siguiente proceso:

Aprobaciones externas necesarias antes de comenzar las tareas: Sor Zoila Pacheco, rectora

Aprobaciones internas necesarias antes de contactar a los contratistas: Lcdo. Pedro Auz, Lcda. Mariana Collaguazo

Procedimientos para obtener las aprobaciones en situaciones de emergencia:

Identificación del estado de desastre potencial:

Una de las primeras tareas es determinar si la crisis actual o latente es lo suficientemente grave como para requerir la evacuación del personal. El servicio de Auditoría cuenta con una sola puerta de salida hacia el corredor del edificio central de la Institución “Fray Saturnino Gutiérrez”. Los demás aspectos son los mismos enunciados en el Servicio de Admisión.

Involucrar a los servicios de emergencia:

En el Servicio de Auditoría está encabezado por el Lcdo. Pedro Auz y la Lcda. Mariana Collaguazo, acompañados por la Lcda. Dorita Gómez, Lcda. Myriam Chiluisa, Lcda. Dayana Cabrera, Lcda. Magali Valdez. Este equipo además proveerá asistencia en el terreno si se requiere otro tipo de especialistas.

Evaluar el impacto potencial de la emergencia en el negocio:

Lo expuesto en el Servicio de Admisión

Movilizar al equipo de recuperación del desastre:

Lo expuesto en el Servicio de Admisión

Notificación a los gerentes y empleados clave:

Esta sección del PCN conoce que los empleados claves de esta sección son el Lcdo. Pedro Auz y la Lcda. Mariana Collaguazo y el gerente principal se mantiene la Rectora Sor Zoila Pacheco. El listado del personal clave de este Servicio y el resto de servicios se detallan en el capítulo 6.

El registro de los eventos, el manejo de la información a los padres de familia, proveedores y público en general, así como la notificación a los familiares será manejado en idéntica forma como se describe en el Servicio de Admisión.

Personal responsable de las actividades de recuperación de las instalaciones y los datos de contacto ante emergencias: Ing. Patricio Martínez

Personal responsable de aprobar las reparaciones o reemplazos de los equipos, muebles y los datos de contacto ante emergencias: Lcdo. Pedro Auz.

7.2. Fase de Recuperación del Negocio

La fase de recuperación del negocio podrá seguir directamente tanto a la fase de recuperación del desastre como iniciarse luego de una emergencia grave que afecte a las operaciones normales del negocio que no hayan dado lugar a una fase de recuperación del negocio. La fase de recuperación del negocio implica la restauración de las operaciones normales del negocio luego de un evento inesperado que interrumpió todos o parte de los procesos de negocio. Desde la perspectiva del proyecto, esta fase es crítica para el PCN. La eficiencia y eficacia de los procedimientos que forman parte de esta sección pueden tener una incidencia directa en la habilidad de la Institución para sobrevivir. Este parte del capítulo de Responsabilidades del Riesgo está relacionado en primer lugar con el proceso de recuperación del colegio y luego con los procedimientos a seguir para restaurar cada uno de los servicios individuales. Una tarea significativa durante la fase de recuperación del negocio es la evaluación del daño a la propiedad, sus contenidos y los sistemas.

7.2.1. Movilización del Equipo de Recuperación del Negocio

Inmediatamente después de una emergencia que afecta seriamente a uno o más procesos normales de la Institución, se debe notificar al Equipo de Recuperación del Negocio (BRT). En caso de que sea necesaria una fase de recuperación del desastre inicial, el BRT debe quedar en espera. Si no hay fase de recuperación del desastre o la fase de recuperación del desastre está por concluirse, se convocará al BRT al centro de comando de la emergencia en cuyo caso este centro de comando estaría dispuesto en las oficinas del Rectorado de la Institución, lugar desde donde se manejará tanto el proceso de emergencia como el de recuperación.

Se puede considerar apropiado incluir un procedimiento de estados de alerta de 3 niveles, como por ejemplo:

- Estado amarillo: DRT en alerta de espera
- Estado anaranjado: DRT en alerta
- Estado rojo: movilización del DRT

El equipo de recuperación del negocio estaría constituido por cada uno de los ADP de los procesos en estudio, con su correspondiente auxiliar en caso de que el primero faltase por alguna circunstancia:

EQUIPO DE RECUPERACIÓN DEL NEGOCIO		
SERVICIO	ADP	AUXILIAR
Admisión	Lcda. Ana Cobos	Srta. Carolina Yamberla
Colecturía	Lcda. Norma Lincango	Srta. Ana Pacheco
Mantenimiento y Reparación	Lcdo. José Luis Rodríguez	MSc. Juan Carlos Cobos
Académico	Lcda. Guadalupe Tituaña	Lcda. Viviana Abata
Gestión Humana	Lcda. Yolanda Yáñez	Ing. Patricio Martínez
Auditoría	Lcdo. Pedro Auz	Licda. Mariana Collaguazo

7.2.2. Evaluación del daño e impacto en la Institución

Una vez que el Equipo de Recuperación del Negocio (BRT) se movilizó, la primera tarea es la evaluación de la extensión del daño y el impacto en el proceso de negocio. Esta actividad debe enfocarse en el impacto en el negocio, en oposición a la evaluación del daño que lleva a cabo el Equipo de recuperación del desastre que está principalmente enfocado en el impacto en las personas y la infraestructura física.

El efecto del desastre será revisado, analizando cada uno de los Servicios que son objeto del presente estudio, si el impacto es total, consideramos pertinente realizar la revisión del impacto siguiendo la prioridad estudiada a lo largo del proyecto.

Esta sección del PCN debe contener una lista de las áreas del colegio y los Servicios afectados por el desastre. Se deben listar las dependencias cruzadas de los procesos afectados con otros procesos. Para cada Servicio afectado deberá haber una estimado preliminar del tiempo de recuperación necesario para restablecer las operaciones normales.

Se incluye en el PCN un formulario para la evaluación del daño que utiliza el BRT.

Tipo de Desastre	Consecuencia	Impacto	Solución	Tiempo

7.2.3. Plan específico de recuperación

A continuación de la fase de evaluación del impacto en el negocio, se necesita preparar un Plan de recuperación. Todo esto se irá preparando una vez que el evento disruptivo haya ocurrido. Inicialmente, esto será un plan resumido ya que el requerimiento más importante será movilizar los recursos para la recuperación lo más rápidamente posible. Sin embargo, con el objeto de ser efectivo. El proceso de estar planificado y estructurado cuidadosamente y el responsable del Equipo de recuperación del negocio debe ser un experto en planificación, organización y en la toma de decisiones bajo condiciones extremas.

El plan de recuperación identifica aquellas áreas que necesitan ser tratadas inmediatamente y establece una secuencia de prioridades de cómo proceder en el proceso de recuperación. Las actividades deben realizarse en forma simultánea siempre que sea posible, pero debe identificarse un camino crítico cuyas actividades deben tener asegurada la prioridad más alta.

El plan de recuperación lista las actividades que necesitan llevarse a cabo según la secuencia de prioridad y qué personas o equipos son responsables de completarlas. En caso de que sea necesario que proveedores y vendedores suministren productos o servicios como parte del proceso de recuperación en estas actividades, entonces deben estar involucrados.

El plan de recuperación activa el proceso de recuperación junto con las personas y los equipos de trabajo.

El Equipo de recuperación del negocio está totalmente dedicado a cubrir el alcance de la operación de recuperación y las actividades que deben llevar a cabo. El impacto de cada una de sus tareas en el camino crítico debe ser comunicado.

Para cada Servicio de la Institución el plan de recuperación podría seguir el siguiente orden

SERVICIO	
Resumen del Plan:	
Recursos a ser movilizados:	1. 2. 3.
Áreas de Tratamiento Inmediato:	1. 2. 3.
Prioridades:	1. 2. 3.
Actividades:	1. 2. 3.
Equipo:	

Proveedores y Vendedores:	1. 2.
Responsable:	

7.2.4. Monitoreo del Servicio

Es necesario que el líder del BRT monitoree de cerca el proceso de las tareas individuales de recuperación durante esta fase. Las dificultades vividas por un grupo de personas pueden tener un efecto significativo en otras tareas dependientes. Es importante también asegurar que cada tarea tiene los recursos apropiados y que los esfuerzos requeridos para establecer la operación normal del negocio no fueron subdimensionados.

7.2.5. Mantener a todos informados

Durante la fase de recuperación del desastre es extremadamente importante que las personas y la Institución como tal se mantengan totalmente informadas. Esto incluye:

- Servicio de Admisión
- Servicio de Colecturía
- Servicio de Mantenimiento y Reparaciones
- Servicio Académico
- Servicio Gestión Humana
- Servicio de Auditoría
- Personal
- Clientes
- Empresas de seguro
- Proveedores y vendedores
- Personal contratado

Un área particularmente importante a considerar es notificar a los clientes, entendiéndose padres de familia y estudiantes, además del personal docente y administradores acerca del impacto en la entrega de los servicios de la Institución. Ellos deberán ser los primeros en ser considerados al notificar sobre los daños ocurridos. La demora en tiempo que tendrá la recuperación del Servicio. Y se les señalará los métodos alternativos para la provisión de los bienes, sobre todo si estos son críticos y pueden afectarlos radicalmente. El cliente expuesto deberá mantenerse informado del progreso del proceso de recuperación. Las estimaciones de tiempo de las operaciones normales deben ser anunciadas con cuidado por cada uno de los Servicios.

Una vez que se restauraron las operaciones normales del negocio, será necesario devolver la responsabilidad de las operaciones específicas a los responsables habituales de cada uno de los

Servicios de la Institución. Este proceso debe formalizarse para asegurar que todas las partes entienden el cambio. Es posible que durante el proceso de recuperación, la responsabilidad general esté asignada al líder del proceso de recuperación del negocio, los cuales serían los ADP de cada proceso y que fueron cubiertos al inicio de la sección de la fase de recuperación del negocio. Inevitablemente, los responsables habituales van a estar involucrados a lo largo de todo el proceso. Pero para que el proceso de recuperación sea totalmente efectivo, la responsabilidad general durante ese período estará en el Equipo de recuperación el negocio.

7.2.6. Reporte de la fase de recuperación del negocio

Una vez completada la fase de recuperación del negocio, cada ADP, particularmente aquel del servicio afectado debe preparar un reporte de las actividades realizadas, así:

SERVICIO:	
Evento ocurrido:	
Personal notificado:	
Fecha de notificación:	
Acciones aplicadas:	
Resultados obtenidos:	
Evaluación:	

7.3. Actividades de Recuperación del Negocio

Esta sección del PCN contiene una lista de los procedimientos a seguir para alcanzar un proceso de recuperación coherente y estructurado. Debe notarse que el nivel de severidad de la emergencia puede afectar a la manera en que los Servicios del colegio son implementados.

La plantilla del PCN también contiene un formato adecuado para registrar los roles y responsabilidades de los miembros individuales de los Servicios. Estos formularios permitirán que las expectativas del Equipo de recuperación del negocio sean comunicadas en forma apropiada a cada miembro del Servicio.

7.3.1. Suministro eléctrico

Esto requiere normalmente la participación de los proveedores de los servicios, los ingenieros de mantenimiento, especialistas técnicos externos y personal de mantenimiento interno de las instalaciones. Si bien dentro de este aspecto debería contemplarse el servicio de gas y agua potable, sin embargo remitiremos este trabajo sobre el servicio eléctrico, ya que la mayor parte se requiere el uso del suministro eléctrico para el buen funcionamiento de los Servicios. Para volver al normal funcionamiento si la falla está en el suministro interno, la Institución recurre a la revisión de los elementos de alimentación de energía propia, para ello se encargará el Sr. Segundo

Guamán, con el apoyo del Arquitecto Jaimes. Si la falla está en el servicio externo del suministro, los responsables constituyen la Empresa Eléctrica de la ciudad de Quito.

7.3.2. Sistema de Comunicaciones

Si los equipos de comunicación han sido dañados durante la emergencia será necesario repararlos o reemplazarlos. Para lo cual la institución busca entre los distintos proveedores de comunicaciones la oferta más adecuada para obtener el equipo dañado, pero la habilitación del sistema de comunicación está a cargo del Consejo Nacional de Telecomunicaciones (CNT), quienes enviarán al experto externo para volver al normal funcionamiento.

7.3.3. Sistemas de la Tecnología de la Información

Si el equipo de sistemas de IT se dañó durante la emergencia, deberá ser reparado o reemplazado. Incluye, todos los equipos propios o utilizados por la Institución. Para ello el órgano regular consiste en comunicar al Servicio de Mantenimiento y Reparaciones sobre el daño del equipo, a través del Lic. José Luis Rodríguez, este comunica inmediatamente al Lcdo. Juan Carlos Cobos quien se encarga de presentar el problema a la rectora Sor Zoila Pacheco para autorizar el presupuesto necesario, una vez autorizado el mismo inmediatamente el Lcdo. Cobos se contacta con el proveedor, que en el caso de la Institución es Tecno Mega, quien provee el equipo requerido.

7.3.4. Recursos Humanos

Durante un incidente particularmente grave, es necesario poner énfasis especial en el bienestar de los empleados ya que pueden estar sujetos a situaciones de estrés inusuales. El ADP del Servicio de Gestión Humana, Lcda. Yolanda Yáñez deberá poner especial énfasis en aquellos empleados en extremo susceptibles y que requieran un tratamiento especial para ser reportados a los psicólogos de la Institución, particularmente a su principal la Dra. Gabriela Serrano.

7.3.5. Información y documentación

La información y documentación es muy importante en la Institución. Entonces, es importante discernir si esta información sufrió algún daño. Si el daño se extendió a la información computarizada u otro tipo de información, se recomienda concentrarse inicialmente en los registros vitales esenciales. Siempre que sea posible, como buena práctica se recomienda que en la Institución los registros vitales sean duplicados y guardados en un lugar off-site de modo que la pérdida permanente no sea un problema real. El lugar off-site de la Institución lo constituiría la Casa de las Hermanas Dominicas de Santa Catalina de Siena.

7.3.6. Operaciones y administración

Esta parte requiere una consideración especial luego de una interrupción a los procesos de negocio normales. Es importante que los clientes, docentes, personal administrativo afectados estén al tanto de las circunstancias y los esfuerzos que se están realizando para restaurar las operaciones normales. Para ello la persona encargada de la comunicación de los avances será el líder del PCN, Ing. Patricio Martínez, un presupuesto preliminar del Plan de Continuidad de Negocios como tal se explica a continuación, se añade además los sub presupuestos y el Presupuesto Total Final:

PRESUPUESTO DEL PCN POR SERVICIO

		Cantidad	P. Unitario	P. Total
	SERVICIO DE ADMISION			
1.	Hardware			
1.1	Ángulos y faceplate	2	35,15	70,30
1.2	Impresora a color Samsung CLP300	1	160,00	160,00
1.3	Tester de red Nexxt para RJ - 45, RJ - 11, RJ - 12	1	29,99	29,99
1.4	UPS BE 450G-LM	1	61,61	61,61
2.	Software			
2.1	Ad Aware Personal Firewall 3.0	1	27,95	27,95
2.2	Administrador		500,00	500,00
2.3	Aplicación de contraseñas	Mensual	10,00	10,00
2.4	Mantenimiento Continuo	Mensual	35,00	35,00
2.5	Progama de sistema educativo propio de la Institución		1.000,00	1.000,00
2.6	Respaldo de Información	Mensual	35,00	35,00
2.7	Sistema Detector de Intrusos			
	SUBTOTAL Servicio de Admision		1.894,70	1.929,85
	SERVICIO DE COLECTURÍA			
1.	Hardware			
1.1	Ángulos y faceplate	8	35,15	281,20
1.2	UPS BE 450G-LM	1	61,61	61,61
2.	Software			
2.1	Ad Aware Personal Firewall 3.0	1	27,95	27,95
2.2	Administrador		500,00	500,00
2.3	Aplicación de contraseñas	Mensual	10,00	10,00
2.4	Mantenimiento Continuo	Mensual	35,00	35,00
2.5	Programas de sistema contable (TMAX; APOLIO)	1	750,00	750,00
2.6	Respaldo de Información	Mensual	35,00	35,00
2.7	Sistema Detector de Intrusos			
	SUBTOTAL Colecturia		1.454,71	1.700,76

	SERVICIO DE MANTENIMIENTO Y REPARACIONES			
1.	Hardware			
1.1	Ángulos y faceplate	40	35,15	1.406,00
1.1.1	Implementos de Protección	3	3,00	9,00
1.1.2	Organización de cables	13	4,25	55,25
1.1.3	Protectores Plasticos			
1.2	Regletas	10	1,25	12,50
2.	Software			
2.1	Administrador		500,00	500,00
2.2	Hide IP Multi PROXY 1.2	1	161,42	161,42
2.3	Kerios, WinRoute Firewall with Mcafee Server (10 usuarios)	1	240,00	240,00
2.4	Respaldo de Información	Mensual	35,00	35,00
2.5	SNORT GNU libre		-	-
	SUBTOTAL Servicio de Mantenimiento Y Reparaciones		980,07	2.419,17
	SERVICIOS ACADEMICO			
1.	Hardware			
1.1	Ángulos y faceplate	2	35,15	61,61
1.2	UPS BE 450G-LM	1	61,61	61,61
2.	Software			
2.1	Ad Aware Personal Firewall 3.0	1	27,95	27,95
2.2	Administrador		500,00	500,00
2.3	Aplicación de Contraseña	Mensual	10,00	10,00
2.4	División de Servicio			
2.5	Mantenimiento Continuo	Mensual	35,00	35,00
2.6	Respaldo de Información	Mensual	35,00	35,00
2.7	Sistema Detector de Intrusos			
	SUBTOTAL Servicio Academico		704,71	731,17

	SERVICIO DE GESTION HUMANA			
1.	Hardware			
1.1	UPS BE 450G-LM	6	160,00	960,00
1.2	Ángulos y faceplate	12	35,15	421,80
1.3	Servicio de Red OHNK 300			
2.	Software			
2.1	Ad Aware Personal Firewall 3.0	6	27,95	167,70
2.2	Administrador		500,00	500,00
2.3	Aplicación de contraseñas	Mensual	10,00	10,00
2.4	Configurar un PC como servidor principal	1	175,00	175,00
2.5	Mantenimiento Continuo	Mensual	35,00	35,00
2.6	Respaldo de Información	Mensual	35,00	35,00
2.7	Sistema Detector de Intrusos			
	SUBTOTAL Gestión Humana		978,10	2.304,50
	SERVICIO DE AUDITORIA			
1	Aplicación de contraseñas	Mensual	10,00	10,00
2	Mantenimiento Continuo	Mensual	35,00	35,00
3	Respaldo de Información	Mensual	35,00	35,00
4	Administrador		500,00	500,00
	SUBTOTAL Auditoria		580,00	580,00
	TOTAL		6.592,29	9.665,45
	LICENCIAMIENTO CORPORATIVO EMPRESA INTERGRUPO			
	Licencia Windows 7 Pro			125,37
	Licencia Office 2007 Estándar			197,62
	TOTAL			322,99

SUBPRESUPUESTOS:

ADMISIÓN			COLECTURÍA			MANTENIMIENTO Y REPARACIONES		
PRESUPUESTO INICIAL			PRESUPUESTO INICIAL			PRESUPUESTO INICIAL		
1.	Materiales	1200	1.	Materiales	6400	1.	Materiales	2200
	Teconológicos	2020		Teconológicos	1060		Teconológicos	10179
2.	Humanos	800	2.	Humanos	800	2.	Humanos	1100
<i>Subtotal</i>		4020	<i>Subtotal</i>		8260	<i>Subtotal</i>		13479
<i>5% Imprevistos</i>		201	<i>5% Imprevistos</i>		413	<i>5% Imprevistos</i>		673,95
TOTAL INICIAL:		3819	TOTAL INICIAL:		7847	TOTAL INICIAL:		12805,05
PRESUPUESTO PARA EL PCN			PRESUPUESTO PARA EL PCN			PRESUPUESTO PARA EL PCN		
1.	Hardware	321,9	1.	Hardware	342,81	1.	Hardware	1482,75
2.	Software	1607,95	2.	Software	1357,95	2.	Software	936,42
TOTAL PCN:		1929,85	TOTAL PCN:		1700,76	TOTAL PCN:		2419,17
PRESUPUESTO TOTAL:		5748,85	PRESUPUESTO TOTAL:		9547,76	PRESUPUESTO TOTAL:		15224,22
ACADÉMICO			GESTIÓN HUMANA			AUDITORÍA		
PRESUPUESTO INICIAL			PRESUPUESTO INICIAL			PRESUPUESTO INICIAL		
1.	Materiales	750	1.	Materiales	1350	1.	Materiales	700
	Teconológicos	2420		Teconológicos	1540		Teconológicos	6050
2.	Humanos	1400	2.	Humanos	1200	2.	Humanos	1100
<i>Subtotal</i>		4570	<i>Subtotal</i>		4090	<i>Subtotal</i>		7850
<i>5% Imprevistos</i>		228,5	<i>5% Imprevistos</i>		204,5	<i>5% Imprevistos</i>		392,5
TOTAL INICIAL:		4341,5	TOTAL INICIAL:		3885,5	TOTAL INICIAL:		7457,5
PRESUPUESTO PARA EL PCN			PRESUPUESTO PARA EL PCN			PRESUPUESTO PARA EL PCN		
1.	Hardware	123,22	1.	Hardware	1381,8	1.	Hardware	290
2.	Software	607,95	2.	Software	922,7	2.	Software	290
TOTAL PCN:		731,17	TOTAL PCN:		2304,5	TOTAL PCN:		580
PRESUPUESTO TOTAL:		5072,67	PRESUPUESTO TOTAL:		6190,00	PRESUPUESTO TOTAL:		8037,5
PRESUPUESTO FINAL POR SERVICIO:								49821,00
Microsoft Windows 7 Pro			125,37	Total Estaciones:		31	Costo:	3.886,47
Microsoft Office 2007 Estándar			197,62	Total Estaciones:		31	Costo:	6.126,22
TOTAL LICENCIAMIENTO A TRAVÉS DE LA EMPRESA INTERGRUPO S.A.:								10.012,69
PRESUPUESTO TOTAL FINAL:								59.833,69

Se incluye además, un análisis de pérdidas cuantitativas del riesgo más crítico de los diferentes servicios en caso de desastre, según la evaluación de probabilidad e impacto, un ejemplo de esto lo constituye el servicio de admisión el que se describe en la tabla que viene a continuación:

PROBABILIDAD (Escala del 1 al 5)	IMPACTO	BIEN EN RIESGO	COSTO U.S.D.
5	Demora en entrega de reportes. Reportes mal elaborados.	Aplicaciones de Office 2007	254,19
		Sistema de Notas	1000,00
		McAfee antivirus	524,19
4	Entrega de valores falsos al Ministerio de Educación	Archivos con información relevante sobre notas u otros.	604,09
3	Estudiantes y padres de familia mal informados. Preocupación académica por información mal entregada	Matriz de comunicación.	447,22
		Teléfonos y otros dispositivos de comunicación.	
3	Pérdida de datos e información sensible. Daños en los dispositivos electrónicos, muebles de madera o similares.	Equipo electrónico: computador, regulador de voltaje y máquinas de escribir Impresoras.	651,60
		Muebles de madera y bodega del segundo nivel	2267,52
TOTAL			5748,81

8. PROTECCION

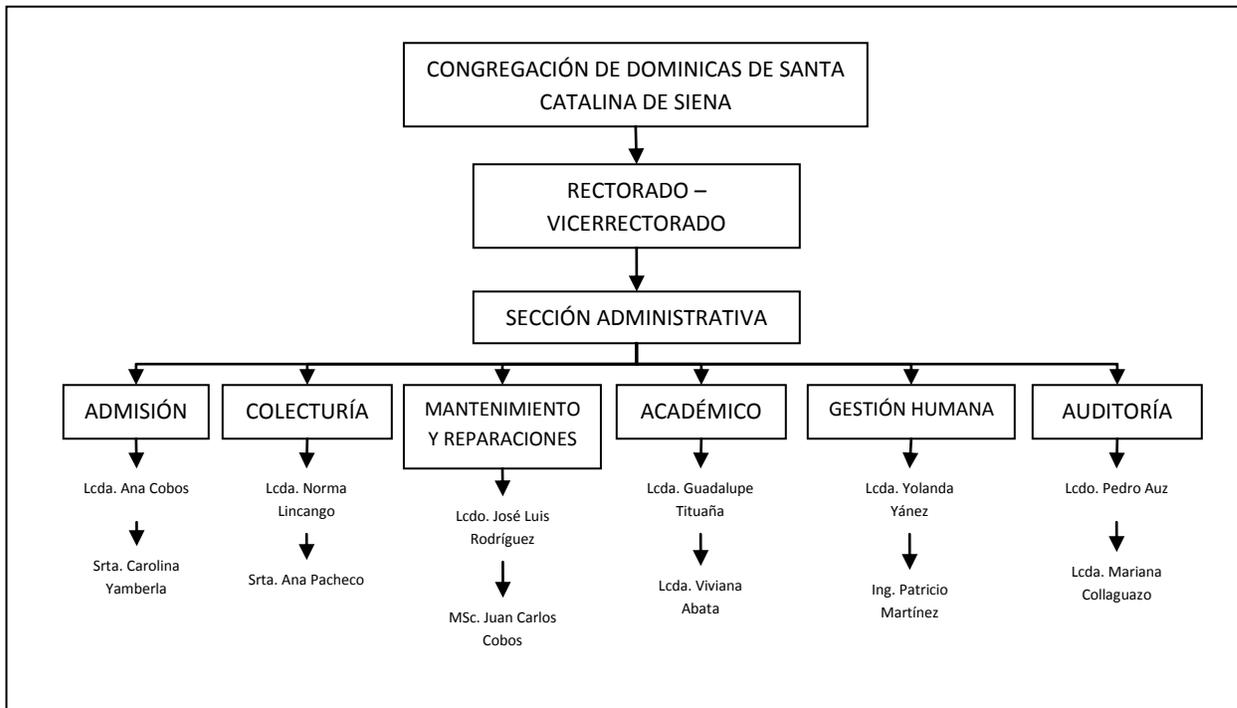
Una vez que se completaron los procesos de iniciación del proyecto y se evaluaron los riesgos del negocio, es necesario tomar medidas para minimizar los efectos de las emergencias potenciales. El objetivo subyacente de este capítulo es identificar los modos de evitar que una emergencia se convierta en un desastre para la organización. El foco está en aquellas actividades de negocio claves para que sea viable la continuidad del mismo.

Todas las organizaciones deben prepararse para posibles situaciones de emergencia y deben considerar qué tipo de estrategias preventivas y de backups son apropiadas para cada aspecto de las actividades del negocio. Esta sección del PCN discute las opciones disponibles de estrategias y se basa en la evaluación de riesgos del negocio que se llevó a cabo en los capítulos anteriores.

La complejidad y los costos asociados a los procedimientos y sistemas de backups dependerán de la velocidad con que los sistemas o los procesos de negocio deben restaurarse. En general, el costo es el factor principal en la velocidad de recuperación, y un sitio backups despejado será significativamente más costoso de instalar y mantener que un proceso manual.

8.1. Organigrama funcional

El PCN debe contener información sobre la estructura funcional de la organización. En la Institución este incluye los nombres de todos los ADP y el personal clave. Esta información es necesaria para identificar las responsabilidades y dependencias que son útiles en los primeros momentos de la emergencia. El Organigrama de la Obra Educativa (basados en los servicios estudiados):



8.2. Estrategias de backups y recuperación de los sistemas IT

Para la mayor parte de las organizaciones, uno de los aspectos más importantes del PCN consiste en elegir la estrategia apropiada para la recuperación de los sistemas IT. La Unidad Educativa “Nuestra Señora del Rosario” no es la excepción al respecto, pero los costos como hemos venido enfatizando pueden ser en extremo alto si la selección requiere una alta asignación de presupuesto.

En la Institución procuramos relacionar los procesos de negocio claves con los sistemas IT y la velocidad de recuperación de la estrategia seleccionada. Hemos considerado el impacto de un daño potencial severo tanto a las instalaciones como a los sistemas de comunicación que puede, a su vez, impactar en los servicios y sistemas IT de la Obra Educativa. Dos de los factores más importantes que consideramos son la criticidad de los sistemas IT para los procesos de negocio (la velocidad necesaria de recuperación) y la cantidad de dinero disponible para las estrategias de backups y recuperación de IT.

Hemos procurado determinar las estrategias de backups y recuperación para la información y documentación crítica. Actualmente nuestros Servicios son totalmente dependientes de la disponibilidad de la información digitalizada para funcionar. Para ello hemos identificado estas dependencias y tratar de desarrollar estrategias de trabajo como medida satisfactoria para continuar las operaciones aún cuando la interrupción haga extremadamente difícil o incluso imposible el acceso a esa información. Si bien es verdad que la Institución cuenta con discos duros externos como apoyo para realizar backups de respaldo, sin embargo, no mantienen una política adecuada para realizar los respaldos a la información, probablemente cada Servicio procuraría

independientemente manejar una política de respaldo individual, ya que como hemos visto cada Servicio tiene su propio administrador para la parte de la IT, sin embargo, hemos considerado importante acordar una misma forma de backups con el objeto de que así todos los Servicios cumplan con idénticas especificaciones al momento de obtener un respaldo digitalico, el mismo que se explica a continuación:

1. No tiene discusión de que la forma más eficiente y menos propensa a errores y descuidos consiste en nombrar un responsable de copias de seguridad que sea el encargado de realizarlas:
 - Admisión: Lcda. Ana Cobos
 - Colecturía: Lcda. Norma Lincango
 - Mantenimiento y Reparaciones: Ing. Juan Carlos Cobos
 - Académico: Lcda. Guadalupe Tituaña
 - Gestión Humana: Ing. Patricio Martínez
 - Auditoría: Lcdo. Pedro Auz
2. Todos ellos adoptarán la política de almacenar la información en ubicaciones específicas, para ello se ha dispuesto en el Servidor Proliant ML 150G6, un espacio de almacenamiento hacia donde irá la información a respaldar. Además, otros lugares de almacenamiento de las copias de seguridad serán:
 - Para los Servicios de Admisión y Académico: disco duro externo que será ubicado en archivadores metálicos en la Casa Parroquial de las Hermanas Dominicanas de Santa Catalina de Siena.
 - Para el Servicio de Colecturía: disco duro externos que deberá ubicarse en el mismo archivador metálico en la misma Casa Parroquial.
 - Para el Servicio de Mantenimiento y Reparaciones: deberá guardar en discos duros externos, CD de apoyo ya que es el encargado de salvaguardar la información del servidor, por ende la información será encriptado a través del Steganos Password Manager y almacenado en el mismo archivador metálico de la Casa Parroquial.
 - Para los Servicios de Gestión Humana y Auditoría: disco duro externo que será almacenado en un lugar especial del domicilio del líder del PCN.

Estos discos duros externos son almacenados cerca del lugar donde serán necesarias, para conseguir restaurar en el menor tiempo posible un sistema afectado por algún tipo de desastre. Hemos convenido también que los discos serán dispuestos en los propios Servicios únicamente en las mañanas mientras realizamos los períodos normales de trabajo, una vez concluida la labor serán llevados a la “Casa Parroquial de las Hermanas Dominicanas”, donde serán ubicados en otro lugar seguro, procurando que el mismo sea un armario ignífugo. Lugar de acceso físico no autorizado, propiedad exclusiva de las hermanas de la Comunidad.

3. Para las copias, hemos considerado el siguiente esquema de trabajo: el lunes se realiza la copia de seguridad completa de todo el sistema, incluido como es obvio todo lo

desarrollado durante el día señalado. Al final de la jornada del martes se realiza una copia diferencial, en la que sólo se copian los archivos que se han cambiado a lo largo del día respecto de la copia de seguridad completa del lunes. Al final del miércoles se realiza otra copia diferencial, en la que se copian los archivos que han cambiado durante ese día, pero se vuelven a copiar los que cambiaron el martes. Jueves se realiza otra copia diferencial que contenga los archivos que cambiaron el martes y miércoles. Como puede verse, a medida que transcurre la semana, las copias diferenciales almacenaran cada vez más información. Lo mismo ocurrirá con el día jueves y el día viernes. Este sería el último día de nuestra semana laboral, e igual como lo señalamos en el numeral anterior, serán trasladadas las copias en disco duro externo a la Casa Parroquial ya descrita. En todo caso, si ocurriera un desastre, por ejemplo, en jueves, se tomaría la copia completa del lunes y las copias diferenciales de martes y miércoles, con ello restauraríamos la máquina al estado en el que estuvo el miércoles por la noche. Estamos consciente que es un método lento y ocupa más espacio a las horas de realizar las copias. Sin embargo, tarda mucho menos tiempo en restaurarlas. Y si fallan martes o miércoles, el sistema podría seguir restaurándose completamente. Este sistema de respaldo será idéntico para todos los Servicios con el único afán de que mantengamos una “sincronía” en el respaldo de la información y con ello procurar generar un hábito de trabajo.

4. La información a copiar sería:

- Información del sistema: archivos del sistema operativo y software instalado.
- Información del usuario: datos generados por las aplicaciones, documentos de Office, registros de nuestras bases de datos, información de servidores WEB, etc.

Por ello, hemos de mantener en lugar seguro copias de respaldo de los sistemas operativos y de las diversas aplicaciones utilizadas en la Institución, lo referente a la información del usuario fue claramente enfocado en el numeral 3 del presente capítulo.

8.3. Cobertura de Seguro

Una estrategia importante para considerar es el mantenimiento de una cobertura de seguro por pérdidas inesperadas ante una emergencia. Hay agentes de seguros especializados capacitados para evaluar si una cobertura de seguro es adecuada para situaciones específicas.

La cobertura de seguro debe considerarse para los edificios y otras instalaciones, los costos incurridos debido a la emergencia, pérdida de ingresos, acciones de la autoridad civil, reclamos de los clientes y otras partes por mal funcionamiento y otras pérdidas potenciales resultantes, la empresa encargada de la cobertura en este tipo de problemas es la Compañía Ecuatoriana de Seguros S.A. También se debe considerar asegurar al personal clave, por ello para los estudiantes, personal docente, administrativo y de servicio se cuenta con la aseguradora Raúl Coka Barriga cuyos detalles se observan en el Anexo 5.

8.4. Proveedores y personal clave del PCN

Los empleados de la Obra Educativa son el activo más importante y valioso. En caso de emergencia, además de recuperar los sistemas, la organización depende de sus empleados para poder recuperar las operaciones de negocio normales en un período de tiempo mínimo. También dependerá de sus proveedores principales de insumos y servicios críticos para recuperar la operación normal de la Institución.

Su Plan de Recuperación de Desastres (DRT) y su PCN dependen principalmente de los miembros del personal y de los ADP que poseen las habilidades técnicas y de gestión necesarios para lograr una recuperación calma del negocio. Una estructura bien organizada evitará que una crisis inesperada devenga en un caos.

8.4.1. Equipo de Recuperación del Desastre

Será necesario establecer un Equipo de recuperación de desastre para manejar la situación inicial de emergencia. Sin embargo, por lo expuesto está claro que la Institución tendrá definido ya este equipo. Estará compuesto por un grupo de especialistas previamente nominados que estén disponibles para asistir en la emergencia inicial. Estas no tienen por qué ser las mismas personas del Equipo de recuperación del negocio. Durante la emergencia inicial el personal a continuación puede llegar a estar involucrado, dependiendo de las circunstancias:

Miembros clave del gerenciamiento:

- Gerente del PCN: Ing. Patricio Martínez
- Gerentes de instalaciones y edificios: Lcdo. José Luis Rodríguez
- Técnico gerente en IT: MSc. Juan Carlos Cobos
- Técnico gerente en comunicaciones: Ing. Fausto Chinlle
- Personal de seguridad: Dr. Orlando Paredes
- Oficial de seguridad de la información: Lcda. Guadalupe Tituaña

El Equipo de recuperación del desastre trabajará en conjunto con los servicios de emergencia en despejar la situación de crisis y emergencia inicial de modo que el Equipo de recuperación del negocio pueda iniciar sus actividades. El DRT sólo podrá iniciar sus actividades de recuperación una vez que los servicios de emergencia hayan dado permiso al comienzo de las actividades. Durante la emergencia inicial, el DRT estará disponible para brindar asistencia a los servicios de emergencia. La configuración del DRT dependerá de tipo y nivel de seguridad de la emergencia.

Los miembros nominados del DRT deben estar disponibles en cualquier momento y asegurar que sus datos de contacto son conocidos por los servicios de emergencia, los datos de este personal han sido incluidos a lo largo del proyecto. Todos los miembros del Equipo de recuperación del desastre deben mantener una copia actualizada del PCN en un lugar seguro off-site.

8.4.2. Equipo de Recuperación del Negocio

La Institución ha establecido un Equipo de recuperación del negocio dedicado formado por los ADP de cada servicio y personal de operaciones encargado de implementar los procedimientos de recuperación necesarios una vez que ocurrió la emergencia. Un miembro senior del nivel gerencial de la organización debe liderar al equipo de recuperación del negocio (BRT), cuya responsabilidad recae en el dueño del PCN señor Patricio Martínez. En caso de una emergencia de ese calibre, el líder del BRT será el encargado de llevar a cabo todo el proceso y asegurar que la organización retorne a la operación normal lo más pronto posible.

Cada miembro del BRT debe tener una copia actualizada del PCN en un lugar seguro off-site y debe estar familiarizado con su contenido. Los detalles en cuanto a su conformación están incluidos en el sub capítulo referente a Movilización del Equipo de Recuperación del Negocio.

8.5. Procedimientos y documentación clave

8.5.1. Documentos y registros vitales de procesos de la Institución

El PCN debe contener información sobre documentos y registros considerados esenciales para la viabilidad del colegio. Existen muchos documentos de este estilo en la Institución y el Equipo del PCN ha decidido que los documentos que son realmente claves para la recuperación del proceso en caso de emergencia, se ubiquen en el Servicio de Documentación (no analizado en el presente proyecto) a cargo de la Lcda. Cecilia Chiluisa, que son parte del Servicio de Gestión de Calidad que procura el colegio.

8.5.2. Almacenamiento fuera de la Institución

Se considera la necesidad de guardar copias de los documentos, información y sistemas claves fuera de las oficinas centrales. Parte de la estrategia de recuperación y backups implica asegurar copias de los registros y documentos vitales en lugares alternativos y seguros.

Esta sección del PCN contiene información sobre los lugares de almacenamiento off-site utilizados por la Institución, incluyendo dirección y números de contacto. También se deben incluir las instrucciones sobre cómo acceder al mismo durante una emergencia, los nombres y números de contacto del personal responsable del la guarda de dichos registros y datos, esto es:

SERVICIO	SITIO OFF - SITE	NOMBRE DEL CONTACTO	NÚMERO DEL CONTACTO
Admisión	Casa Dominicas Santa Catalina de Siena	Sor Zoila Pacheco	023342476
Colecturía	Casa Dominicas Santa Catalina de Siena	Sor Zoila Pacheco	023342476
Mantenimiento y Reparaciones	Casa Dominicas Santa Catalina de Siena	Sor Zoila Pacheco	023342476
Académico	Casa Dominicas Santa Catalina de Siena	Sor Zoila Pacheco	023342476
Gestión Humana	Pomasqui	Patricio Martínez	022351464
Auditoría	Pomasqui	Patricio Martínez	022351464

8.5.3. Procedimientos para el manejo de padres de familia, proveedores y público en general

Se debe considerar una estrategia adecuada a seguir para manejar las preguntas de padres de familia, proveedores y público. Es normal mantener la política de que sólo el personal específicamente autorizado tiene permiso para hablar con los medios. Esta regla es particularmente importante durante las condiciones de emergencia.

La organización debe entonces seguir una política adecuada al respecto. Adicionalmente, esta sección incluye una lista del personal autorizado, recayendo esta responsabilidad en la Lcda. Guadalupe Tituaña, y como personal auxiliar la responsabilidad está en la Lcda. Viviana Abata.

8.5.4. Autorización para la protección en caso de emergencia

Cada una de las personas autorizadas para la protección en caso de emergencia fueron analizadas a lo largo del capítulo de responsabilidades de riesgo, es importante añadir que en el sistema de protección debe considerarse que en una situación de emergencia, los procedimientos normales de autorización pueden quedar sin efecto, ser demasiado lentos ante una urgencia o las personas autorizadas para tomar decisiones fundamentales pueden no estar disponibles. Los procesos de autorización ante emergencias necesitan estar establecidos para permitir que se lleven a cabo los trabajos de recuperación sin demoras innecesarias.

Es extremadamente importante que los procedimientos formen parte del PCN y que los trabajos de recuperación y restauración de los servicios ocurran a la mayor brevedad posible.

9. CAPACITACIÓN DEL PERSONAL

Todo el personal debe ser capacitado en el proceso de recuperación del negocio. Esto es particularmente importante cuando los procedimientos son significativamente diferentes de los que se utilizan en la operación normal. Esta capacitación será integrada en la fase de capacitación general o tratada por separado. La misma se planificará cuidadosamente y se brindará de manera estructurada. Será evaluada para verificar que haya alcanzados los objetivos y es relevante para los procedimientos involucrados y se dará utilizando únicamente los recursos internos debido a los costos asociados.

9.1. Gestión del Proceso

Para que la fase de capacitación del PCN sea exitosa debe estar bien gestionada y estructurada. Será necesario identificar el objetivo y alcance de la capacitación, qué capacitación específica es requerida, quiénes asistirán a la misma y preparar un presupuesto para los costos adicionales asociados a esta fase en la siguiente forma para la Institución:

9.1.1. Objetivos y Alcance

El PCN debe contener una descripción de los objetivos y el alcance de la fase de capacitación. Esto permitirá que la capacitación sea consistente y organizada de manera que los resultados sean mensurables y la capacitación se ajuste de manera apropiada. El alcance seguirá el modelo establecido a través del S.M.A.R.T. en el texto Administración Profesional de Proyectos de Yamal Chamoun⁷, lo que significa que será Específico, Medible, Acordado, Realista y en el Tiempo previsto.

Objetivo del PCN para la Obra Educativa “Nuestra Señora del Rosario”.

Entrenar al personal en los procedimientos particulares a seguir durante el proceso de recuperación del negocio para regresarlos a la normalidad en el menor tiempo posible y siguiendo una estructura adecuada contemplada en el PCN

Alcance del PCN para la Obra Educativa “Nuestra Señora del Rosario”.

La capacitación debe llevarse a cabo de manera detallada y exhaustiva para que el personal se familiarice con todos los aspectos del proceso de recuperación. La capacitación cubre todos los aspectos de la sección de actividades de recuperación del negocio del PCN incluyendo la recuperación de los sistemas de IT

⁷ CHAMOUN, Y. (2007): Administración Profesional de Proyectos. México D.F.: Ed. McGraw Hill.

Se intentará desarrollar un programa para generar conciencia corporativa y comunicar los procedimientos para el proceso de recuperación del negocio

9.1.2. Necesidades de la Capacitación

Las personas seleccionadas para este proceso serán todos los ADP de los Servicios e incluso los Jefes de Área de las asignaturas que se imparten en la Institución con el objetivo de procurar una concientización plena incluso en los estudiantes y las estudiantes. Se dará un Manual que explique en forma sucinta todo lo detallado en el presente proyecto, este manual de procedimiento deberá ser explicado de tal forma que sea comprendido por las personas que requieren llevarlos a cabo. Como la institución no es una organización en extremo grande, se contemplará la elaboración de talleres de trabajo, sobre los que se repartirán diferentes temas del PCN para que sean analizados y emitir juicios de valor que vayan en apoyo del PCN.

9.1.3. Material de capacitación

Una vez que las necesidades de capacitación fueron identificadas, es necesario especificar y desarrollar el material de capacitación adecuado. Esta actividad pueden llevar mucho tiempo, por lo tanto al menos que se les dé prioridad a los programas de capacitación críticos, puede demorar el hecho de que la organización alcance un nivel de preparación adecuado. Inicialmente se ocupará el Manual descrito en el párrafo anterior y el material añadido saldrá de los talleres explicados.

9.1.4. Agenda preliminar de capacitación

Una vez que se acordó que es necesaria una capacitación y que los materiales para la misma están listos, se debe desarrollar una agenda de capacitación detallada:

Mes: Agosto

Fecha: Lunes 23 al viernes 27

Hora: 8:00 hasta las 13:45 horas

Lugar: Biblioteca de la Institución

Asistentes: ADP de Servicios y Jefes de Área

Tema general: Plan de Continuidad de Negocios aplicado en el ámbito educativo.

9.1.5. Comunicación

Una vez organizada la capacitación a los empleados, es necesario comunicarles la agenda de los programas que se acordaron. Esta sección del PCN contendrá un borrador de la comunicación a enviar a cada miembro del personal para ponerlo al tanto de la agenda de trabajo. La comunicación espera una respuesta de los miembros del personal confirmando si asistirán en la fecha convenida. Se le dará información a cada miembro del personal sobre su rol y sus responsabilidades en caso de emergencia.

COMUNICACIÓN

Quito, agosto del 2010

Servicio:

ADP o Jefe de Área: Lcdo.

De mi consideración:

A través de la presente se le hace conocer acerca de la necesidad de la Obra Educativa “Nuestra Señora del Rosario” de contar con su asistencia al curso sobre PLAN DE CONTINUIDAD DE NEGOCIO EN EL ÁMBITO EDUCATIVO, cuyo taller iniciará el día lunes 23 de agosto hasta el viernes 27 del mismo mes, a partir de las 8:00 horas hasta las 13:45, a cargo del Ing. Patricio Martínez, para reforzar la calidad de la institución y contar con un plan que nos permita regresar lo más pronto posible al normal desenvolvimiento de nuestras actividades en caso de presentarse alguna emergencia de cualquier índole y mantener de la mejor forma nuestra Certificación de la Calidad ISO 9001 – 2008.

Por su gentil atención le reitero mi sincero agradecimiento.

Atentamente,

Sor Zoila Pacheco

RECTORA

P.D.: Solicitamos confirmar su asistencia a través del presente comunicado, caso contrario designar a un miembro de su equipo para que acuda al Curso.

9.2. Evaluación de la Capacitación

Los programas individuales de capacitación y todos los procesos generales de capacitación del PCN serán evaluados para asegurarnos que han sido efectivos y aplicables. Esta información será distribuida entre los capacitadores y los asistentes para que completen los cuestionarios de retroalimentación.

9.2.1. Cuestionarios

Es vital recibir retroalimentación de los ADP y de los jefes de área que participarán en cada uno de los programas de capacitación del PCN. Esto permitirá identificar y eliminar las debilidades del proceso de recuperación del negocio o de la capacitación.

Completar los formularios de feedback es mandatorio para todas las personas que participen en el proceso de capacitación. Los formularios deben completarse durante la capacitación (para registrar algún tema en particular) o inmediatamente terminada la práctica. Esto permitirá documentar las observaciones y comentarios mientras el evento está todavía reciente en la mente de las personas.

La Institución cuenta con un formulario específico creado dentro del colegio durante el tiempo de obtención de la Certificación ISO, el mismo que está estructurado de la siguiente forma:

EVALUACIÓN DE LA CAPACITACIÓN

LUGAR Y FECHA:
 TEMA DE LA CAPACITACION:
 DURACIÓN:
 AREA A CAPACITARSE:

TOME EN CUENTA LA SIGUIENTE ESCALA

- 5 Excelente
- 4 Muy bueno
- 3 Bueno
- 2 Satisfactorio
- 1 Regular

Marque con una X en la columna que a su juicio refleje lo ocurrido en el desarrollo de la capacitación

Nº	FACTORES	5	4	3	2	1
1	CUMPLIMIENTO DE LOS OBJETIVOS					
2	DESEMPEÑO DE LOS INSTRUCTORES					
3	CALIDAD DEL MATERIAL DIDACTICO					
4	SATISFACCIÓN DE EXPECTATIVAS					
5	INTEGRACIÓN GRUPAL					
	TOTAL					

Marque con una X en la columna que a su juicio evalúe la labor del instructor

Nº	FACTORES	5	4	3	2	1
1	PREPARACIÓN DE LA MATERIA IMPARTIDA					
2	CUMPLIMIENTO DE LOS OBJETIVOS					
3	CUMPLIMIENTO DEL PROGRAMA					
4	DOMINIO DE LA MATERIA					
5	CAPACIDAD DE ENSEÑAR					
6	USO DE AYUDAS DIDÁCTICAS					
7	INTERACCIÓN ENTRE INSTRUCTOR Y PARTICIPANTES					
8	LENGUAJE VERBAL UTILIZADO					
9	SEGURIDAD Y SINCERIDAD					
10	PUNTUALIDAD Y ASISTENCIA					
	TOTAL					

SUGERENCIAS

a.- QUE ASPECTOS CONSIDERA DEBEN SER MEJORADOS RESPECTO A LA ORGANIZACIÓN DE LA CAPACITACIÓN

b.- DESCRIBA EN FORMA CONCRETA LOS ASPECTOS POSITIVOS OBSERVADOS EN EL DESARROLLO DE LA CAPACITACIÓN

MUESTRA:

Firma del Responsable

9.2.2. Evaluación de la retro alimentación

Los cuestionarios completos de los asistentes a la capacitación y el feedback de los capacitados deben evaluarse. Las debilidades identificadas deben notificarse al líder del Equipo del PCN para fortalecer el proceso según corresponda.

Los temas claves mencionados por los asistentes deben ser tomados en cuenta y considerar si son críticos o no para el proceso. Si hay un número significativo de ítems negativos encontrados entonces se debe considerar el hecho de realizar la capacitación nuevamente una vez que los materiales de capacitación o el proceso sean mejorados.

10. PRUEBAS DE VALIDACIÓN

El PCN debe ser testeado dentro de un ambiente realista, lo cual significa simular las condiciones que van a aplicar a una emergencia actual. También es importante que el test se lleve a cabo con las personas que serán responsables de esas actividades ante una crisis.

10.1. Planificación de las pruebas

Esta sección del PCN contempla el establecimiento de los objetivos y el alcance de las pruebas y permite que la fase de prueba esté estructurada y organizada adecuadamente.

10.1.1. Objetivos y alcance de las pruebas

El PCN en estudio contiene una descripción de los objetivos y el alcance de la fase de prueba. Esto permite que las pruebas se estructuren y se organicen de manera que los resultados puedan medirse y el plan se ajuste lo necesario, así:

Objetivo de las pruebas del PCN para la “Obra Educativa Nuestra Señora del Rosario”.

Llevar adelante una prueba rigurosa del proceso de recuperación del negocio, incluyendo la simulación del evento disruptivo, resultados obtenidos que puedan ser mensurables y evaluados en forma conjunta y aprovecharlos para modificar el PCN y mejorarlo.

Alcance del PCN para la “Obra Educativa Nuestra Señora del Rosario”.

Las pruebas se llevan a cabo de manera detallada y exhaustiva de modo que todos los aspectos del plan puedan probarse. Las pruebas deben estar respaldadas, de manera significativa, por todas las unidades de negocio y soporte dentro de la organización. Las pruebas incluyen la recuperación de todos los aspectos de la sección del PCN de Actividades para la recuperación del negocio incluyendo los sistemas IT

10.1.2. Ambiente de las pruebas

Uno de los desafíos más importantes de las pruebas del proceso de recuperación del negocio es crear condiciones reales para llevar adelante las pruebas. En la Institución se ha creado un sistema de evacuación en caso de un temblor, terremoto o incendio, coadyuvado por el Servicio Médico, cuyo plan se expone a continuación:

Basados en el objetivo del plan de seguridad Institucional y siguiendo el PCN que se pretende establecer, la prueba contra desastres naturales mantiene los siguientes lineamientos:

- 1.- Permitir, limitar y reducir los efectos del sismo, incendios u otros.
- 2.- Alcanzar una eficiente organización, capacitación y adiestramiento del personal a fin de que cuando se presente la emergencia reaccione inmediata y eficazmente.

Aprobación:



Rectora de la Institución: Obra Educativa
"Nuestra Señora del Rosario"

Sor. Zoila Pacheco.

Fecha:

Mes:	Día.	Hora.

Listado general del personal del establecimiento.

Número de Profesores.	51
Número del personal administrativo.	13
Número del personal directivo.	3
Número del personal médico.	3
Número del personal DOBE	3
Número del personal de apoyo.	5
Número de Alumnos	1142

Comité Institucional ante emergencias.

Primeros Auxilios:	Dra. Martínez Jenny
Campamentación:	Lcdo. Jaime Landeta
Orden y Seguridad.	Lcdo. Victor Orellana
Contra Incendios.	Lcda. Viviana Abata
Búsqueda rescate y evacuación.	Lcdo. Carlos Venegas
Comunicación.	Lcda. Ana Cobos
Amplificación.	Lcdo. Angel Puruncajas

EJECUCIÓN:

1. Unidad de Evacuación.



Poner en ejecución todas las actividades previstas con su respectivo jefe de unidad

1.1. Personal encargado:

Jefe de Unidad: Lcdo. Carlos Venegas.

1.2. Docentes:

Sección básica, sección secundaria.

Guiar a los estudiantes evacuados en forma ordenada, manteniendo calma a la zona de

seguridad establecida.

Cada docente tutor se encargará de guiar a su paralelo en la sección básica el momento de la evacuación, realizar el control tomando lista de su respectivo grado con el fin de verificar la presencia de todos sus estudiantes.

Y para la sección diversificada en paralelo el docente que esté dando su cátedra, será responsable de sus estudiantes en el momento de la evacuación, tomando lista de su respectivo curso con el fin de verificar la presencia de todos sus estudiantes.

2. Unidad de orden y seguridad.

Poner en ejecución todas las actividades previstas en el plan.

2.1. Personal encargado:

Jefe de Unidad: Lcdo. Victor Orellana.

Comunicar a todos los docentes de cada paralelo, el día, la hora, toque de alarma para la ejecución del simulacro. Colaborando en la coordinación con la alarma y su codificación

Alarma corta = evacuación interna.
Alarma continua = evacuación externa.

Inspector sección básica: Lcdo. Carlos Venegas

Inspectora sección secundaria: Lcda. Karina Godoy

3. Unidad de Primeros Auxilios.



Proporcionar primeros auxilios a evacuados cuando necesiten, hasta que llegue el personal, equipo y medios especializados, que realicen la evacuación hasta las instalaciones hospitalarias.

3.1. Personal encargado:

Jefe de Unidad: Dra. Jenny Martinez.

3.2. Departamento médico odontológico.

Odontólogo: Orlando Paredes.

Auxiliar: Janet Medrano.

3.3. DOBE (Departamento de Orientación y Bienestar Estudiantil):

Yolanda Yáñez.

Gabriela Serrano

Doris Rea.

El personal debe mantener un botiquín de Primeros Auxilios, cuyo material se explica en el Anexo 6.

4. Unidad Contra Incendios u otros.



Mantener el orden en los puntos críticos del edificio y no permitir el acceso a ellos especialmente durante la evacuación.

Asegurar el establecimiento evacuado y la zona de seguridad.

Cuidar los bienes del establecimiento, antes, durante y después a fin de evitar que se cometan actos vandálicos.

4.1. Personal encargado:

Jefe de unidad: Lcda. Viviana Abata.

- Lcda. Cecilia Chiluisa.

- Lcda. Susana Vargas.
- Lcdo. Cesar Simbaña.
- Lcda. Paulina Moreta.
- Lcdo. Angel Puruncajas.

5. Unidad de Comunicación.

Mantener informados a familiares sobre la situación. Establecer contactos con los organismos básicos.

5.1. Personal encargado:

Jefe de unidad: Lcda. Ana Cobos.

- Srta. Carolina Yamberla
- Lcda. Sandra Revelo

6. Unidad de Campamento y Refugios.



Ubicar y organizar la zona de seguridad, que proporcione adecuada protección y seguridad a los estudiantes evacuados. Recibir, clasificar y atender heridos, enfermos, extraviados etc., en la zona de seguridad.

6.1. Personal encargado:

Jefe de unidad: Lcdo. Jaime Landeta.

- Lcdo. Jorge Reyes.

- Lcdo. Carlos Jurado.
- Lcdo. Oswaldo Peña.
- Lcda. Sandra Giron.
- Lcda. Mónica Herrera.
- Lcda. María Simbaña
- Lcdo. Fausto Poveda
- Sra. Gloria Erazo
- Sr. Segundo Guamán
- Sra. Rosario Salinas

Responsable: _____ Firma _____

Esta sección del PCN, en el caso anterior, ha demostrado tener una lista útil en caso de una emergencia en caso de cualquier desastre natural. La Institución con el PCN desarrollado ha generado su propia lista de modo de asegurar que sea la adecuada para su situación particular y las circunstancias pronosticadas como potenciales emergencias. Listas explicadas a lo largo del presente proyecto.

En el **Servicio de Admisión:**

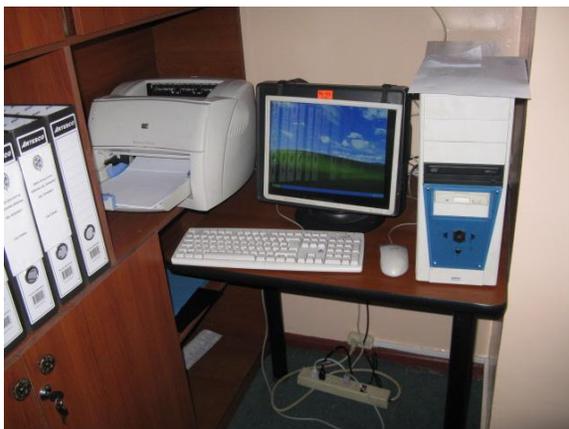


Riesgo: Crimen cibernético, actos de sabotaje, fallos en los sistemas de comunicación y fallos en el sistema de electricidad.

Luego de desarrollar el PCN toda la información importante se almacena en archivadores metálicos y se incluyó toda la información importante en discos duros externos que son trasladados a la Casa Parroquial una vez concluida las labores de trabajo.



En el **Servicio de Colecturía:**



Riesgo: Fallos en el sistema de electricidad, robo y fallos en el sistema de conducción.

Luego del desarrollo del PCN se añadió UPS de protección, alarmas contra robos y archivadores de madera con mayores seguridades.



En el **Servicio de Mantenimiento y Reparaciones:**

Riesgo: Crimen cibernético, fallos en el sistema de electricidad y actos de sabotaje





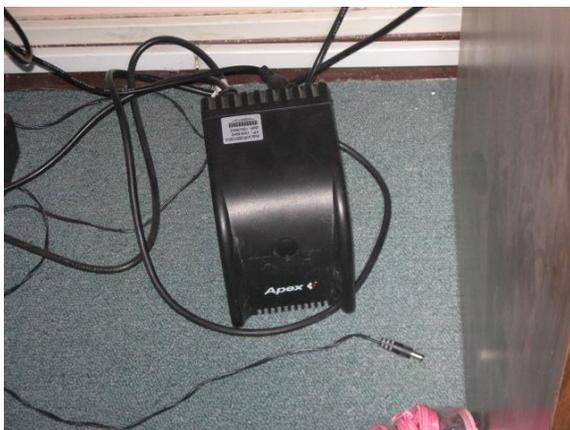
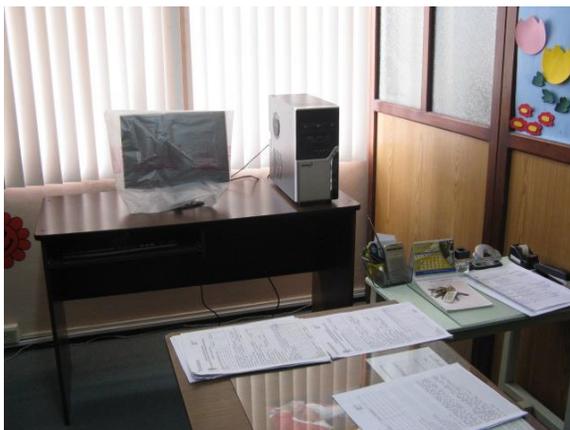
Los alambres se encuentran completamente sueltos lo que aumenta el riesgo de incendios.



Posterior a la aplicación del PCN se adquirió un servidor con mejores características de trabajo, así mismo se colocó extintores próximo a la zona, incluso dentro del mismo salón, así también se colocó una jaula de protección para el UPS.

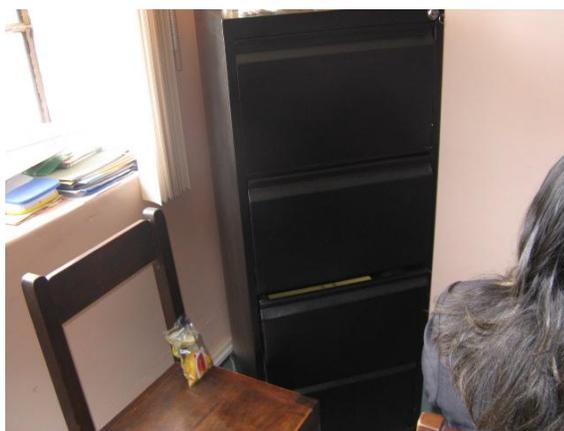


En el Servicio de Gestión Humana:



Riesgo: Crimen cibernético, actos de sabotaje, robo, revelación de información sensible, fallos en el sistema de electricidad.

Luego del PCN se colocó la información sensible en archivadores metálicos, se realizaron reuniones periódicas para una mejor capacitación del personal, se realizó respaldos semanales de la información en discos duros externos y se añadió extintores en zonas cercanas.





En el **Servicio de Auditoría:**



Riesgos: básicamente la revelación de información sensible, actos de sabotaje y en igual medida el crimen cibernético.

Sin embargo es importante considerar que mucho del trabajo realizado para esta área vino de parte de la Curia Diocesana quien tomo las medidas que serían apropiadas para el PCN, entre ellas incluye el uso de regletas de protección para los alambres, en idéntica forma un servidor adecuadamente custodiado desde la misma Curia.

A ello hemos añadido la capacitación incluso a los mismo estudiantes sobre el manejo de los instrumentos tecnológicos.



10.1.3. Conducción de las pruebas

Para asegurar la consistencia del proceso de pruebas en la Institución, uno o más miembros del Equipo del PCN debe ser el encargado de coordinar los procesos de prueba dentro de cada servicio y a lo largo de toda la Institución.

Cada Servicio debe probarse en forma completa y el coordinador debe asegurar que cada Servicio contempla las reglas necesarias asociadas para asegurar que el proceso de prueba está siendo llevado a cabo dentro de un ambiente real.



Nuestro PCN ya ha nombrado a quienes serán miembros del Equipo del PCN candidatos para coordinar el proceso de prueba. Así también se ha listado las responsabilidades de los coordinadores en los capítulos previos. Favor revisar el capítulo de Protección.

Por otro lado, con el objeto de asegurar que los resultados medidos son consistentes, las pruebas deben monitorearse en forma independiente. Esta tarea normalmente es llevada a cabo por un miembro del Equipo de

recuperación del negocio o del Equipo BCP, que como se mencionó consta en el capítulo referente a Protección.

10.1.4. Retroalimentación

Es vital recibir retroalimentación de las personas que están manejando y participando en cada una de las pruebas. Esta retroalimentación permite identificar y eliminar las debilidades del proceso de recuperación del negocio. Completar los formularios de retroalimentación es mandatorio para todas las personas que participen del proceso de prueba. Los formularios deben completarse durante la prueba (para registrar un problema particular) o inmediatamente después de concluido. Esto permitirá registrar las observaciones y comentarios mientras el evento sigue fresco en la cabeza de la gente.

10.1.5. Presupuesto para la fase de prueba

Cada fase del proceso PCN que incurre en un costo requiere que se prepare y se apruebe el presupuesto. La fase de preparación para una posible emergencia del proceso PCN involucra la identificación e implementación de las estrategias para el backups y la recuperación de los

archivos de datos o una parte del proceso de negocio. Es inevitable que estos procesos de backups y recuperación impliquen costos adicionales. Las partes críticas del proceso de negocio como los sistemas IT pueden requerir la implementación de estrategias particulares de backups costosas.

Si los costos son significativos deben ser aprobados con el detalle del presupuesto en forma separada del establecimiento y los costos de funcionamiento y mantenimiento.

10.1.6. Capacitación

Con el objeto de que el proceso de prueba se lleve a cabo sin incidentes, es necesario que el equipo de prueba esté capacitado en procedimientos de emergencia. Esto probablemente sea mejor de manejar en un ambiente de taller de trabajo y debe ser presentado por las personas responsables de desarrollar los procedimientos de emergencia.

Es importante que se den instrucciones claras al equipo de prueba, considerando las condiciones de simulación que se deben tener en cuenta. La capacitación fue explicada en el capítulo previo.

10.2. Conducción de las pruebas

Las pruebas deben llevarse a cabo en condiciones reales y todos los participantes deben tomar el proceso seriamente. Es importante que todas las personas que posiblemente estén involucradas en la recuperación particular de un proceso de negocio en caso de emergencia, participen en el proceso de prueba. Debe ser mandatario que el ADP de cada Servicio esté presente cuando se llevan a cabo las pruebas de su área.

Siempre y cuando sea práctico, se debe probar por completo cada parte crítica del proceso de recuperación del negocio. Cada parte de los procedimientos incluidos en el proceso de recuperación debe ser testeado para asegurar su validez y relevancia.

Durante el proceso de prueba se deben reconfirmar los números de contacto en caso de emergencia de los empleados y proveedores. Todos los números de contacto de los empleados involucrados deben validarse. Esto es particularmente importante para el manejo de los empleados claves que son críticos para alcanzar el éxito del proceso de recuperación. Esta actividad suele llevarla a cabo el área de Gestión Humana en nuestra Institución.

Si la emergencia ocurre fuera del horario normal de trabajo, se deberá contactar a un gran número de personas. Se puede utilizar un método jerárquico donde una persona contacta a otras cinco o un método en cadena donde el llamado se realiza de uno en uno.

Este proceso debe tener incorporado alguna cláusula para asegurar que en caso de no poder contactar a una persona por alguna razón, se registre y se notifique al responsable a cargo. Esto permitirá utilizar rutas de contacto alternativas.

10.2.1. Evaluación de los resultados de las pruebas

Prepare una evaluación general del resultado de las pruebas para cada proceso de negocio. Las siguientes preguntas son ejemplos a tomar en cuenta:

- Si se alcanzaron los objetivos del proceso de recuperación de la Institución. En caso contrario, comentar.
- Si las condiciones simuladas eran razonablemente “reales”. En caso contrario, comentar.
- Si los datos de prueba eran representativos. En caso contrario, comentar.
- Si las pruebas se llevaron a cabo sin inconvenientes. En caso contrario, comentar.
- Cuáles son los comentarios principales que se recibieron a través de los cuestionarios de retroalimentación.

Cada prueba debe ser evaluada como totalmente satisfactoria, adecuada o que requiere una prueba adicional.

11. MANTENIMIENTO

Al igual que otras Instituciones, la Obra Educativa “Nuestra Señora del Rosario” vive cambios todos los tiempos. El aumento de los procesos basados en tecnología en los últimos diez años y particularmente los últimos cinco, trajo aparejado a la Institución un aumento del nivel de dependencia de la disponibilidad de los sistemas y la información para que el negocio funcione de manera efectiva. Estos cambios van a continuar y la única certeza es que el ritmo de cambio se seguirá incrementando. Es necesario que el PCN aplicado en el colegio siga este ritmo de cambio para que sea útil en caso de una emergencia disruptiva.

Es necesario que el PCN esté estructurado y controlado adecuadamente para facilitar el proceso de actualización. Siempre que se generen cambios al PCN deben probarse completamente y hacer las modificaciones necesarias en el material de capacitación.

Esto implica el uso de procedimientos formales de control de cambio a cargo del líder del Equipo PCN.

11.1. Control de cambio

Se recomienda implementar controles de cambio formales para cubrir las modificaciones requeridas al PCN. Esto es necesario, debido al nivel de complejidad del PCN. Se debe preparar y aprobar una solicitud de cambio para cada modificación propuesta al PCN. A continuación se expone un modelo que será de utilidad dentro de la obra:

OBRA EDUCATIVA “NUESTRA SEÑORA DEL ROSARIO”

FORMULARIO DE SOLICITUD DE CAMBIO

Nº de solicitud:	Cliente:	Fecha:	Hora:
Persona de Contacto:	Aplicación:	Dirigido al técnico:	Fecha Servicio:
Descripción de la Modificación:			
Motivo de la Modificación:			
Firma del Cliente:			
Fecha:			
Aprobado por:			

11.2. Responsabilidades de mantenimiento

Cada parte del plan se asigna a un miembro del Equipo del PCN quien estará a cargo de actualizar y mantener el plan. El líder del Equipo del PCN mantendrá el control general del PCN pero cada ADP de cada Servicio deberá mantener las secciones del PCN correspondientes a sus áreas actualizadas todo el tiempo.

Es importante que los responsables del PCN y del Equipo de recuperación del negocio estén totalmente informados de todo cambio aprobado del plan.

11.3. Pruebas de mantenimiento

El Equipo del PCN de la institución nombra a cada ADP como responsable de las pruebas de mantenimiento y de asegurar que todos los cambios al plan se prueben adecuadamente. Siempre que se realice o se proponga un cambio al PCN, se notificará al responsable de pruebas del PCN, que en el caso de la Obra es el líder del PCN. Esta persona será, a su vez, responsable de notificar a todos los Servicios afectados y de acordar cualquier otra actividad de prueba.

11.4. Responsable de capacitación

El líder del Equipo del PCN notifica al coordinador de capacitación del PCN Lcda. Yolanda Yáñez, ADP de Gestión Humana todos los cambios aprobados al PCN para que se actualicen los materiales de capacitación. Se debe evaluar si los cambios ameritan una nueva capacitación tal como se describió en el capítulo anterior.

12. CONCLUSIONES

Al desarrollar el PCN se logró concientizar a todo el personal que labora en la institución con el fin de que estén prestos, para que cuando ocurra algún incidente en cualquiera de los servicios críticos vuelva a su normal funcionamiento en el menor tiempo posible, aplicando lo establecido en el PCN.

El establecimiento de políticas aumentó entre los empleados el reconocimiento del impacto, que un incidente serio podría causar en la Institución, lo que permitió definir un presupuesto inicial para dar a conocer exactamente cuales activos y que valor tienen cada uno de ellos dentro de cada servicio, esto generó dentro de la organización la aprobación de los diferentes equipos del proyecto.

La identificación de los riesgos generales y particulares en los servicios críticos así como sus causas, la probabilidad e impacto, permitió establecer los tiempos mínimos que pueden permanecer sin función cualquiera de los servicios.

Los administradores tienen un procedimiento a seguir logrando minimizar o eliminar el riesgo y los tiempos de respuesta ya que se cuenta con un proceso formal establecido.

Los miembros de los equipos de recuperación del desastre y de recuperación del negocio están capacitados en caso de ocurrir un incidente ya sea en horas laborables como en horas no laborables

Queda instituida las políticas de respaldo en la institución por lo que han adquirido una disciplina de protección y respaldo para evitar los problemas de sabotaje y pérdidas.

Los equipos de recuperación de negocios y desastre, a través de los planes del PCN identifican en forma profesional el estado de un desastre potencial, y evalúan el impacto de la emergencia.

El compromiso con el PCN crea la necesidad de estar capacitándose permanentemente, para lo que se ha determinado fechas específicas para las capacitaciones, y los integrantes de la Institución están comprometidos con la elaboración de evaluaciones para ratificar su nexos con el compromiso citado.

Todo el personal de la Institución, a través del conjunto de pruebas y simulacros continuos, adquiere un adecuado adiestramiento para saber específicamente qué hacer en caso de que el desastre se presentara, por lo que queda claramente en su memoria cuáles son las medidas a adoptar para enfrentar cualquier riesgo.

13. RECOMENDACIONES

Estas son las recomendaciones necesarias para mejorar aún más el desarrollo del PCN en la Obra Educativa “Nuestra Señora del Rosario”:

Las Políticas y Procedimientos, deberán ser revisados periódicamente para que vaya acorde con los cambios que se generasen al interior de la Institución.

Se debe definir claramente las responsabilidades de cada miembro del proceso y tener en un lugar visible, permanentemente, cuáles son estos y cuáles sus roles dentro de su Servicio, así ellos estarán continuamente preparados frente a la crisis, con la intención, de que si se cambia de miembros, los nuevos estén considerados y adecuadamente entrenados.

Se puede mejorar aún más la disciplina de protección y respaldo para evitar los problemas de sabotaje y pérdidas, cualquiera que esta fuese la causa, sea por desastre natural, robo o ingeniería social. Para ello definir adecuadamente fechas para capacitar al personal encargado, administradores y demás miembros de los Servicios, Salas de Computación. Esta capacitación debe extenderse al alumnado de la Institución para que también adquieran conciencia de su responsabilidad.

Se debería buscar nuevas capacitaciones para cada integrante de la Institución, con la finalidad de que vayan acorde a los nuevos avances dentro del ámbito del PCN, por lo que se debería realizar cada 3 meses capacitaciones y simulacros, y procurar profesionales en el área para tener un mejor respaldo para el colegio.

Se recomienda generar un fondo económico permanente de apoyo para el PCN, que esté exclusivamente orientado a este Plan.

Finalmente, insistir sobre la creación de un Plan de Concientización sobre la importancia del PCN para la Obra Educativa, y el compromiso de todos los empleados para garantizar su éxito.

14. ANEXOS

14.1. ANEXO 1

14.1.1. NORMA ISO 27002:2005

A continuación se describen en forma sucinta las cláusulas que comprenden:

1. **Políticas de seguridad:** el estándar define como obligatorias las políticas de seguridades documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.
2. **Aspectos organizativos:** establece el marco formal de seguridad que debe integrar una organización.
3. **Clasificación y control de activos:** el análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.
4. **Seguridad ligada al personal:** contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información. Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, o sea, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.
5. **Seguridad física y del entorno:** identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.
6. **Gestión de comunicaciones y operaciones:** integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.
7. **Control de accesos:** habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.
8. **Desarrollo y mantenimiento de sistemas:** la organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.
9. **Gestión de incidentes de seguridad de la información:** este es el nuevo valor añadido a la antigua norma ISO 17799. Se deberían establecer las responsabilidades y procedimientos

de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.

10. **Gestión de continuidad del negocio:** el sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.
11. **Conformidad:** la organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

14.2. ANEXO 2

14.2.1. NORMA ISO 9001 – 2008

El presente anexo incluye únicamente el punto 7 en lo referente a la Norma ISO, aquella relacionada con el PCN.

7. REALIZACIÓN DEL PRODUCTO

7.1. PLANIFICACIÓN DE LA REALIZACIÓN DEL PRODUCTO

La organización debe planificar y desarrollar los procesos necesarios para la realización del producto. La planificación de la realización del producto debe ser coherente con los requisitos de los otros procesos del sistema de gestión de la calidad.

Durante la planificación de la realización del producto, la organización debe terminar, cuando sea apropiado, lo siguiente:

- a) Los objetivos de la calidad y los requisitos para el producto,
- b) La necesidad de establecer procesos y documentos y de proporcionar recursos específicos para el producto,
- c) Las actividades requeridas de verificación, validación, seguimiento, medición, inspección y ensayo/prueba específica para el producto así como los criterios para la aceptación del mismo,
- d) Los registros que sean necesarios para proporcionar evidencia de que los procesos de realización y el producto resultante cumplen los requisitos

El resultado de esta planificación debe presentarse de forma adecuada para la metodología de operación de la organización.

7.2. PROCESOS RELACIONADOS CON EL CLIENTE

7.2.1 Determinación de los requisitos relacionados con el producto

La organización debe determinar:

- a) Los requisitos especificados por el cliente, incluyendo los requisitos para las actividades de entrega y las posteriores a la misma,
- b) Los requisitos no establecidos por el cliente pero necesarios para el uso especificado o para el uso previsto, cuando sea conocido,
- c) Los requisitos legales y reglamentarios aplicables al producto, y
- d) Cualquier requisito adicional que la organización considere necesario.

7.2.2 Revisión de los requisitos relacionados con el producto

La organización debe revisar los requisitos relacionados con el producto. Esta revisión debe efectuarse antes de que la organización se comprometa a proporcionar un producto al cliente (por ejemplo, envío de ofertas, aceptación de contratos o pedidos, aceptación de cambios en los contratos o pedidos) y debe asegurarse de que:

- a) Están definidos los requisitos del producto,
- b) Están resueltas las diferencias existentes entre los requisitos del contrato o pedido y los expresados previamente, y
- c) La organización tiene la capacidad para cumplir con los requisitos definidos

Deben mantenerse registros de los resultados de la revisión y de las acciones originadas por la misma.

Cuando el cliente no proporcione una declaración documentada de los requisitos, la organización debe confirmar los requisitos del cliente antes de la aceptación.

Cuando se cambien los requisitos del producto, la organización debe asegurarse de que la documentación pertinente sea modificada y de que el personal correspondiente sea consciente de los requisitos modificados.

7.2.3 Comunicación con el cliente

La organización debe determinar e implementar disposiciones específicas para la comunicación de los clientes, relativas a:

- a) La información, sobre el producto
- b) Las consultas, contratos o atención de pedidos, incluyendo las modificaciones, y
- c) La retroalimentación del cliente, incluyendo sus quejas.

7.3 DISEÑO Y DESARROLLO

7.3.1 Planificación del diseño y desarrollo

La organización debe planificar y controlar el diseño y desarrollo del producto

Durante la planificación del diseño y desarrollo la organización debe determinar:

- a) Las etapas del diseño y desarrollo
- b) La revisión, verificación y validación, apropiadas para cada etapa del diseño y desarrollo, y
- c) Las responsabilidades y autoridades para el diseño y desarrollo

La organización debe gestionar las interfaces entre los diferentes grupos involucrados en el diseño y desarrollo para asegurarse de una comunicación eficaz y una clara asignación de responsabilidades.

Los resultados de la planificación deben actualizarse, según sea apropiado, a medida que progresa el diseño y desarrollo.

7.3.2 Elementos de entrada para el diseño y desarrollo

Deben determinarse los elementos de entrada relacionados con los requisitos del producto y mantenerse registros. Estos elementos de entrada deben incluir:

- a) Los requisitos funcionales y de desempeño
- b) La información proveniente de diseños previos similares, cuando sea aplicable, y
- c) Cualquier otro requisito esencial para el diseño y desarrollo

Los elementos de entrada deben revisarse para comprobar que sean adecuados. Los requisitos deben estar completos, sin ambigüedades y no deben ser contradictorios.

7.3.3 Resultados del diseño y desarrollo

Los resultados del diseño y desarrollo deben proporcionarse de manera adecuada para la verificación respecto a los elementos de entrada para el diseño y desarrollo, y deben aprobarse antes de su liberación.

Los resultados del diseño y desarrollo deben:

- a) Cumplir los requisitos de los elementos de entrada para el diseño y desarrollo
- b) Proporcionar información apropiada para la compra, la producción y la prestación del servicio
- c) Contener o hacer referencia a los criterios de aceptación del producto, y
- d) Especificar las características del producto que son esenciales para el uso seguro y correcto

7.3.4 Revisión del diseño y desarrollo

En las etapas adecuadas, deben realizarse revisiones sistemáticas del diseño y desarrollo de acuerdo con lo planificado para:

- a) Evaluar la capacidad de los resultados de diseño y desarrollo para cumplir los requisitos, e
- b) Identificar cualquier problema y proponer las acciones necesarias

Los participantes en dichas revisiones deben incluir representantes de las funciones relacionadas con la(s) etapa(s) de diseño y desarrollo que se está(n) revisando. Deben mantenerse registros de los resultados de las revisiones y de cualquier acción necesaria

7.3.5 Verificación del diseño y desarrollo

Se deben realizar la verificación, de acuerdo con lo planificado para asegurarse de que los resultados del diseño y desarrollo cumplen los requisitos de los elementos de entrada del diseño y desarrollo. Deben mantenerse registros de los resultados de la verificación y de cualquier acción que sea necesaria.

7.3.6 Validación del diseño y desarrollo

Se debe realizar la validación del diseño y desarrollo de acuerdo con lo planificado para asegurarse de que el producto resultante es capaz de satisfacer los requisitos para su aplicación especificada o uso previsto, cuando sea conocido. Siempre que sea factible, la validación debe completarse antes de la entrega o implementación del producto. Deben mantenerse registros de los resultados de la validación y de cualquier acción que sea necesaria.

7.3.7 Control de los cambios del diseño y desarrollo

Los cambios del diseño y desarrollo deben identificarse y deben mantenerse registros. Los cambios deben revisarse, verificarse y validarse, según sea apropiado, y aprobarse antes de su implementación. La revisión de los cambios del diseño y desarrollo debe incluir la evaluación del efecto de los cambios en las partes constitutivas y en el producto ya entregado. Deben mantenerse registros de los resultados de la revisión de los cambios y de cualquier acción que sea necesaria.

7.4 COMPRAS

7.4.1 Proceso de compras

La organización debe asegurarse de que el producto adquirido cumple los requisitos de compra especificados. El tipo y el grado del control aplicado al proveedor y al producto adquirido deben depender del impacto del producto adquirido en la posterior realización del producto o sobre el producto final

La organización debe evaluar y seleccionar los proveedores en función de su capacidad para suministrar productos de acuerdo con los requisitos de la organización. Deben establecerse los criterios para la selección, la evaluación y la re – evaluación. Deben mantenerse los registros de los resultados de las evaluaciones y de cualquier acción necesaria que se derive de las mismas.

7.4.2 Información de las compras

La información de las compras debe describir el producto a comprar, incluyendo, cuando sea apropiado:

- a) Los requisitos para la aprobación del producto, procedimientos, procesos y equipos.
- b) Los requisitos para la calificación del personal, y
- c) Los requisitos del sistema de gestión de calidad

La organización debe asegurarse de la adecuación de los requisitos de compra especificados antes de comunicárselos al proveedor.

7.4.3 Verificación de los productos comprados

La organización debe establecer e implementar la inspección u otras actividades necesarias para asegurarse de que el producto comprado cumple los requisitos de compra especificados.

Cuando la organización o su cliente quieran llevar a cabo la verificación en las instalaciones del proveedor, la organización debe establecer en la información de compra las disposiciones para la verificación pretendida y el método para la liberación del producto.

7.5 PRODUCCIÓN Y PRESTACIÓN DEL SERVICIO

7.5.1 Control de la producción y de la prestación del servicio

La organización debe planificar y llevar a cabo la producción y la prestación del servicio bajo condiciones controladas. Las condiciones controladas deben incluir, cuando sea aplicable:

- a) La disponibilidad de información que describa las características del producto
- b) La disponibilidad de instrucciones de trabajo, cuando sea necesario,
- c) El uso de equipo apropiado
- d) La disponibilidad y uso de equipos de seguimiento y medición,
- e) La implementación del seguimiento y de la medición, y
- f) La implementación de actividades de liberación, entrega y posteriores a la entrega del producto.

7.5.2 Validación de los procesos de la producción y de la prestación del servicio

La organización debe validar todo proceso de producción y de prestación del servicio cuando los productos resultantes no pueden verificarse mediante seguimiento o mediciones posteriores y, como consecuencia, las deficiencias aparecen únicamente después de que el producto esté siendo utilizado o se haya prestado el servicio.

La validación debe demostrar la capacidad de estos procesos para alcanzar los resultados planificados.

La organización debe establecer las disposiciones para estos procesos, incluyendo, cuando sea aplicable:

- a) Los criterios definidos para la revisión y aprobación de los procesos,
- b) La aprobación de los equipos y la calificación del personal,
- c) El uso de métodos y procedimientos específicos,
- d) Los requisitos de los registros,
- e) La revalidación.

7.5.3 Identificación y trazabilidad

Cuando sea apropiado, la organización debe identificar el producto por medios adecuados, a través de toda la realización del producto.

La organización debe identificar el estado del producto con respecto a los requisitos de seguimiento y medición a través de toda la realización del producto.

Cuando la trazabilidad sea un requisito, la organización debe controlar la identificación única del producto y mantener registros.

7.5.4 Propiedad del cliente

La organización debe cuidar los bienes que son propiedad del cliente mientras estén bajo el control de la organización o estén siendo utilizados por la misma. La organización debe identificar, verificar, proteger y salvaguardar los bienes que son propiedad del cliente suministrados para su utilización o incorporación dentro del producto. Si cualquier bien que sea propiedad del cliente se pierde, deteriora o de algún otro modo se considera inadecuado para su uso, la organización debe informar de ello al cliente y mantener registros.

7.5.5 Preservación del producto

La organización debe preservar el producto durante todo el proceso interno y la entrega al destino previsto para mantener la conformidad con los requisitos. Según sea aplicable, la preservación debe incluir la identificación, manipulación, embalaje, almacenamiento y protección. La preservación debe aplicarse también a las partes constitutivas de un producto.

7.6 CONTROL DE LOS EQUIPOS DE SEGUIMIENTO Y MEDICIÓN

La organización debe determinar el seguimiento y la medición a realizar y los equipos de seguimiento y medición necesarios para proporcionar la evidencia de la conformidad del producto con los requisitos determinados.

La organización debe establecer procesos para asegurarse de que el seguimiento y medición pueden realizarse y se realizan de una manera coherente con los requisitos de seguimiento y medición.

Cuando sea necesario asegurarse de la validez de los resultados el equipo de medición debe:

- a) Calibrarse o verificarse, o ambos, a intervalos especificados antes de su utilización, comparado con patrones de medición trazables a patrones de medición internacionales o nacionales; cuando no existan tales patrones debe registrarse la base utilizada para la calibración o la verificación;
- b) Ajustarse o reajustarse según sea necesario
- c) Estar identificado para poder determinar su estado de calibración;
- d) Protegerse contra ajustes que pudieran invalidar el resultado de la medición;
- e) Protegerse contra los daños y el deterioro durante la manipulación, el mantenimiento y el almacenamiento.

Además, la organización debe evaluar y registrar la validez de los resultados de las mediciones anteriores, cuando se detecte que el equipo no está conforme con los requisitos. La organización debe tomar las acciones apropiadas sobre el equipo y sobre cualquier producto afectado.

Deben mantenerse registros de los resultados de la calibración y la verificación.

Debe confirmarse la capacidad de los programas informáticos para satisfacer su aplicación prevista cuando éstos se utilicen en las actividades de seguimiento y medición de los requisitos especificados. Esto debe llevarse a cabo antes de iniciar su utilización y confirmarse de nuevo cuando sea necesario.

14.3. ANEXO 3

14.3.1. Entrevista a los Administradores de los Servicios Críticos

ENTREVISTA ADMINISTRADORES DE SERVICIOS CRÍTICOS

Servicio:

Aplicación de Servicio:

Nombre:

Función que desempeña:

Años en la Institución:

Responsabilidades a su cargo:

1. ¿Qué aplicaciones maneja dentro del servicio que usted administra?
2. ¿Cuál considera usted la información más relevante del servicio que administra?
3. Consecuencias de los servicios

Riesgo	Causas	Consecuencias	Probabilidad Ocurrencia	Impacto	Solución

4. ¿Cuáles son los riesgos que usted considera que se ve avocado mayoritariamente, en una escala del 1 al 5?

- Incendio
- Tormentas eléctricas
- Contaminación y amenazas medio ambientales
- Actos de sabotaje
- Robo
- Fallos en el sistema de electricidad
- Fallos en el sistema de comunicación
- Crimen cibernético (malware, hackers, crackers, sniffer, spoofing, etc)
- Pérdida de registros o datos
- Revelación de información sensible
- Fallos en el sistema IT

5. ¿A qué servicios o aplicaciones afectaría si el servicio que usted administra deja de funcionar?
6. ¿Qué tiempo mínimo considera usted que podría pasar sin la información citada?
7. ¿Quién está a cargo del servicio informático cuando usted está de viaje o en clases?
8. ¿Cómo respalda la información a su cargo y con qué periodicidad lo efectúa?
9. ¿Dónde guarda la información respaldada?
10. ¿Qué tipos de seguridad le está configurado a su Servicio?
11. ¿Quién tiene acceso a su información?
12. ¿Cómo está protegida la información de su computadora?
13. ¿Qué programas ayudan en la protección de su información?, ¿conoce usted?, ¿cuáles?
14. ¿Su computadora o servidor donde está alojado el servidor tiene backups del hardware?
15. ¿Tiene servicio de internet?
16. ¿Para qué lo usa frecuentemente?
17. ¿En términos económicos, cuál cree que es el monto aproximado que está a su cargo en general en la administración de servicio?

Considerar que las preguntas 10 y 12 se les solicitaron comedidamente a los administradores del Servicio que se consulte al asistente técnico.

Servicio de Admisión

Aplicación de Servicio: Office 2007, Internet, Sistema de Notas “Nuestra Señora del Rosario”, Programas del Ministerio.

Nombre: Ana Cobos

Función que desempeña: Secretaría General. ADP.

Años en la Institución: 15 años

Responsabilidades a su cargo:

1. ¿Qué aplicaciones maneja dentro del servicio que usted administra? Las señaladas en la aplicación de servicio, particularmente el Sistema de Notas.
2. ¿Cuál considera usted la información más relevante del servicio que administra? Sistemas de Notas, ya que se cubre toda la Obra Educativa, Office debido a la relevancia de ciertos documentos que son de propiedad exclusiva de la Institución y otros que son entregados a los alumnos y alumnas para sus requerimientos particulares. Programas del Ministerio de Educación que nos permite regular el Sistema de Notas mencionado, y en idéntica forma aquellos documentos que son óptimos para el buen desempeño de la Obra Educativa en todos sus ámbitos.
3. Consecuencias de los Servicios.

Riesgo	Causas	Consecuencias	Probabilidad Ocurrencia	Impacto	Solución
Malware	Dispositivos Portátiles	Perdida Información	Continua	Demora en la entrega de reportes	Actualización antivirus IDS Sistema Detector de Intrusos. Firewalls, particularmente AdAware.
Actos de sabotaje	Falsificación de notas Obtención de exámenes	Promoción de un alumno no apto para cursar un nivel superior	Quimestral	Entrega de valores falsos al Ministerio de Educación	Contraseñas con números y símbolos
Fallos en el sistema de comunicación	Mala conducción de electricidad Matriz de comunicaciones mal empleada	Reportes mal elaborados Retraso en la entrega de documentos de soporte	Mensual	Estudiantes y Padres de familia mal informados Preocupación académica por información mal entregada.	Elaboración de matrices de comunicación acorde a las necesidades. Uso de alimentadores continuos de energía.

4. ¿Cuáles son los riesgos que usted considera que se ve avocado mayoritariamente, en una escala del 1 al 5?

- Incendio -----1
- Tormentas eléctricas ----- 2
- Contaminación y amenazas medio ambientales ----- 1
- Actos de sabotaje -----4
- Robo -----1
- Fallos en el sistema de electricidad -----3
- Fallos en el sistema de comunicación -----3
- Crimen cibernético (malware, hackers, crackers, sniffer, spoofing, etc) -----3
- Pérdida de registros o datos -----5
- Revelación de información sensible -----2
- Fallos en el sistema IT -----3

5. ¿A qué servicios o aplicaciones afectaría si el servicio que usted administra deja de funcionar? A toda la organización y desarrollo estudiantil, y particularmente al servicio de notas.

6. ¿Qué tiempo mínimo considera usted que podría pasar sin la información citada? Tiempo máximo de 1 día.

7. ¿Quién está a cargo del servicio informático cuando usted está de viaje o en clases? La Srta. Carolina Yamberla, auxiliar de contabilidad. Ing. Marco Bravo encargado del sistema de notas de la Institución

8. ¿Cómo respalda la información a su cargo y con qué periodicidad lo efectúa? En Disco Duro externo y se lo realiza cada 8 días.

9. ¿Dónde guarda la información respaldada? En la misma oficina el Disco Duro externo y lo referente a información de soporte en la partición D: del mismo computador.

10. ¿Qué tipos de seguridad le están configurados a su Servicio? Contraseñas con referencias familiares o algún elemento institucional. Alarmas de seguridad y de incendio. Antivirus.

11. ¿Quién tiene acceso a su información? En este servicio: la Rectora del plantel, Vicerrectorado, Secretaría, Subdirectora, MSc. Juan Carlos Cobos del Servicio de Mantenimiento y Reparaciones.

12. ¿Cómo está protegida la información de su computadora? A través únicamente de anti – virus y contraseñas.

13. ¿Qué programas ayudan en la protección de su información?, ¿conoce usted?, ¿cuáles? El programa de protección AVG versión 9.0, el cual se maneja únicamente en lo imprescindible sin mayor conocimiento.
14. ¿Su computadora o servidor donde está alojado, el servidor tiene backups del hardware? No posee backups de hardware. La oficina de secretaría está asentada sobre piso de madera, con armarios de madera sintética susceptibles al fuego.
15. ¿Tiene servicio de internet? Si, a través de la empresa CNT (Corporación Nacional de Telecomunicaciones).
16. ¿Para qué lo usa frecuentemente? Se lo usa para la página WEB del colegio: www.colrosario.edu.ec., gráficos requeridos para los docentes, frases para uso de la Institución, contacto con la página del Ministerio de Educación.

17. ¿En términos económicos, cuál cree que es el monto aproximado que está a su cargo en general en la administración de servicio?

Sistema de notas -----	\$ 1000,00
Computadora-----	\$ 300,00
Impresoras -----	\$ 200,00
Muebles y Enseres -----	\$ 1000,00
Máquina de Escribir -----	\$ 200,00
Impresora matricial -----	\$ 300,00
Útiles de oficina-----	\$ 100,00
Archivo muerto -----	\$ 100,00
Regulador de voltaje -----	\$ 20,00
TOTAL: -----	\$ 3220,00

Servicio de Colecturía

Aplicación de Servicio: Office 2007, página WEB del IESS, página del SRI, página del Banco Promérica, Sistema de Contabilidad Olimpo versión 7.0.

Nombre: Lcda. Norma del Pilar Lincango Gualoto CPA.

Función que desempeña: Contadora de la Institución. ADP

Años en la Institución: 1 año.

Responsabilidades a su cargo:

1. ¿Qué aplicaciones maneja dentro del servicio que usted administra? Las señaladas en la aplicación de servicio, particularmente lo referente a las páginas WEB del IESS, SRI, Banco Promérica.
2. ¿Cuál considera usted la información más relevante del servicio que administra? Sistema de Contabilidad Olimpo V7 y todo lo referente a las páginas WEB señaladas.
3. Consecuencias de los Servicios.

Riesgo	Causas	Consecuencias	Probabilidad Ocurrencia	Impacto	Solución
Fallos en el sistema de electricidad	Pérdidas y bajones de electricidad	Daños en los equipos tecnológicos (computadores, impresoras, teléfonos, etc.)	Continua	Perdida de la información contable	UPS Alimentadores continuos de energía. Rehacer la contabilidad.
Robo	Padres de familia inescrupulosos y proveedores	Pérdida de hardware y material tecnológico para el manejo de la información	Semestral	Pérdida de datos y archivos contables.	Sistema de Seguridad más rígido en el control a la entrada y salida de los padres.
Fallos en los sistemas de comunicación	Malá conducción eléctrica	Reporte económico con falencias por mala información	Semestral	Contabilidad defectuosa carente de ciertos términos económicos	Pedir la revisión continua por parte del CNT para mejorar la conducción eléctrica.

4. ¿Cuáles son los riesgos que usted considera que se ve avocado mayoritariamente, en una escala del 1 al 5?

- Incendio -----1
- Tormentas eléctricas ----- 1
- Contaminación y amenazas medio ambientales ----- 1
- Actos de sabotaje -----3
- Robo -----5
- Fallos en el sistema de electricidad -----5
- Fallos en el sistema de comunicación -----4
- Crimen cibernético (malware, hackers, crackers, sniffer, spoofing, etc) -----3
- Pérdida de registros o datos -----1
- Revelación de información sensible -----1
- Fallos en el sistema IT -----1

5. ¿A qué servicios o aplicaciones afectaría si el servicio que usted administra deja de funcionar? Básicamente al cobro de pensiones, pago de sueldos a todo el personal de la Institución, pago de haberes a los proveedores, no se podría cubrir la realización de impuestos.

6. ¿Qué tiempo mínimo considera usted que podría pasar sin la información citada? Un máximo de 2 días.

7. ¿Quién está a cargo del servicio informático cuando usted está de viaje o en clases? La auxiliar de contabilidad Srta. Ana Pacheco

8. ¿Cómo respalda la información a su cargo y con qué periodicidad lo efectúa? No se realiza esta actividad al momento

9. ¿Dónde guarda la información respaldada? En un Disco Duro externo, del que se conoce su existencia, pero no se utiliza adecuadamente. La información únicamente reposa en la computadora a cargo de la responsable de colecturía.

10. ¿Qué tipos de seguridad le están configurados a su Servicio? Básicamente la alarma contra incendios y la alarma contra robos.

11. ¿Quién tiene acceso a su información? Regularmente únicamente la ADP de colecturía y su auxiliar. Remotamente la rectora de la Institución.

12. ¿Cómo está protegida la información de su computadora? Únicamente con antivirus

13. ¿Qué programas ayudan en la protección de su información?, ¿conoce usted?, ¿cuáles? El anti – virus McAfee del que conozco su presencia, más no adecuadamente su uso.
14. ¿Su computadora o servidor donde está alojado, el servidor tiene backups del hardware? No poseemos backups de hardware. La oficina de Colecturía se encuentra alfombrada, con muebles de madera y otros de tabla aglomerada. Posee un pequeño desván donde se guarda suministros de oficina altamente combustibles como papel, papelógrafos, y otros materiales que además son altamente corrosibles.
15. ¿Tiene servicio de internet? Si.
16. ¿Para qué lo usa frecuentemente? Esto permite las transacciones requeridas por la Institución para con el IESS, SRI, Banco Promérica.
17. ¿En términos económicos, cuál cree que es el monto aproximado que está a su cargo en general en la administración de servicio?

Computadoras personales -----	\$ 600,00
Impresora HP Laser -----	\$ 100,00
Impresora EPSON matricial -----	\$ 160,00
Muebles y Enseres -----	\$ 1400,00
Suministros de oficina (aquí se incluye el material del desván que analizamos en la presente descripción -----	\$ 5000,00
Reguladores de voltaje -----	\$ 100,00
TOTAL: -----	\$ 7360,00

Servicio de Mantenimiento y Reparaciones

Aplicación de Servicio: Server 2003, Servicepack 3 XP, Office 2007, Olimpo V7, McAfee, EPO.

Nombre: MSc. Juan Carlos Cobos Velasco

Función que desempeña: Administrador – Técnico

Años en la Institución: 11 años.

Responsabilidades a su cargo:

1. ¿Qué aplicaciones maneja dentro del servicio que usted administra? Las mencionadas en la aplicación de servicios, además de Linux Ubuntu.
2. ¿Cuál considera usted la información más relevante del servicio que administra? Todo lo que se realiza a través de la administración de red, partiendo del Server 2003
3. Consecuencias de los servicios

Riesgo	Causas	Consecuencias	Probabilidad Ocurrencia	Impacto	Solución
Malware	Internet	Pérdida de la información. Servicio de Internet en extremo lento.	Mínimo una vez al año.	Alumnos sin material de trabajo.	Uso de firewalls. IDS. Uso del sistema Linux
Fallos en el sistema de electricidad	Malas conexiones eléctricas. Amontonamiento de los cables en un solo sitio	Peligro de incendio Apagado imprevisto de las computadoras.	Trimestral	Estrés permanente por la falta de protección.	Utilización de una mayor cantidad de dispositivos de conexión para evitar el amontonamiento

4. ¿Cuáles son los riesgos que usted considera que se ve avocado mayoritariamente, en una escala del 1 al 5?

- Incendio -----1
- Tormentas eléctricas ----- 3
- Contaminación y amenazas medio ambientales ----- 1
- Actos de sabotaje -----3
- Robo -----1

- Fallos en el sistema de electricidad -----4
 - Fallos en el sistema de comunicación -----3
 - Crimen cibernético (malware, hackers, crackers, sniffer, spoofing, etc) -----5
 - Pérdida de registros o datos -----2
 - Revelación de información sensible -----2
 - Fallos en el sistema IT -----2
5. ¿A qué servicios o aplicaciones afectaría si el servicio que usted administra deja de funcionar? Todo el servicio administrativo, esto es: Servicio de Admisión y Servicio de Colecturía.
 6. ¿Qué tiempo mínimo considera usted que podría pasar sin la información citada? Tiempo promedio de 2 días.
 7. ¿Quién está a cargo del servicio informático cuando usted está de viaje o en clases? Únicamente el Administrador Técnico, esto es el MSc. Juan Carlos Cobos.
 8. ¿Cómo respalda la información a su cargo y con qué periodicidad lo efectúa? A través de Discos Duros externos, CD de apoyo.
 9. ¿Dónde guarda la información respaldada? En el Servicio de Admisión, es decir, se traslada la responsabilidad al Servicio citado en cuanto a la información de respaldo.
 10. ¿Qué tipos de seguridad le están configurados a su Servicio? Alarma de incendio, alarma de seguridad, firewalls.
 11. ¿Quién tiene acceso a su información? Únicamente el responsable del servicio técnico del Servicio de Mantenimiento y Reparaciones.
 12. ¿Cómo está protegida la información de su computadora? A través de anti – virus y firewalls.
 13. ¿Qué programas ayudan en la protección de su información?, ¿conoce usted?, ¿cuáles? Principalmente McAfee como anti – virus y Zentos como coadyuvante en el apoyo de los firewalls
 14. ¿Su computadora o servidor donde está alojado, el servidor tiene backups del hardware? Posee servicio de backups de hardware a través de su servidor principal. El Servicio de Mantenimiento y Reparaciones en el ámbito técnico se ubica en el Aula de Computo de la Obra Educativa, cuya infraestructura está dada básicamente por piso de madera, paredes de cemento armado, extintor en la pared junto a la puerta de entrada de madera, ya que posee una segunda puerta metálica para el acceso.

15. ¿Tiene servicio de internet? Si, la principal fuente de infecciones en el Servicio
16. ¿Para qué lo usa frecuentemente? Básicamente para servicios de investigación de los estudiantes, además para uso del personal de la institución en el desarrollo de mallas curriculares.
17. ¿En términos económicos, cuál cree que es el monto aproximado que está a su cargo en general en la administración de servicio?

Servidor HP Proliant ML 150G6 -----	\$ 2300,00
Estaciones de trabajo (24 en total) -----	\$ 6000,00
Impresoras -----	\$ 200,00
DSL Wireless HUAWEI Echolife HG520s -----	\$ 50, 00
Switch 3COM Super Stack 3 3C16471 -----	\$ 149,00
Muebles y Enseres -----	\$ 2100,00
Útiles de oficina-----	\$ 100,00
Regulador de voltaje -----	\$ 480,00
UPS APC -----	\$ 100,00
TOTAL: -----	\$ 11479,00

Servicio Académico

Aplicación de Servicio: Sistema operativo Windows XP, Office 2007.

Nombre: Lcda. Guadalupe Tituaña

Función que desempeña: Vicerrectorado y ADP

Años en la Institución: 16 años

Responsabilidades a su cargo:

1. ¿Qué aplicaciones maneja dentro del servicio que usted administra? Básicamente lo que se refiere a material elaborado en Office.
2. ¿Cuál considera usted la información más relevante del servicio que administra? Todo lo que se refiere al manejo de notas por parte de los docentes.
3. Consecuencias de los servicios

Riesgo	Causas	Consecuencias	Probabilidad Ocurrencia	Impacto	Solución
Malware	Dispositivos Portátiles No se actualiza el anti – virus	Perdida de información referente a los planes de los docentes	Dos veces por año	Retraso en el orden cronológico para impartir la cátedra	Actualización continua del anti – virus Uso de IDS Firewall

4. ¿Cuáles son los riesgos que usted considera que se ve avocado mayoritariamente, en una escala del 1 al 5?

- Incendio -----2
- Tormentas eléctricas ----- 3
- Contaminación y amenazas medio ambientales ----- 2
- Actos de sabotaje -----1
- Robo -----2
- Fallos en el sistema de electricidad -----2
- Fallos en el sistema de comunicación -----1
- Crimen cibernético (malware, hackers, crackers, sniffer, spoofing, etc) -----5
- Pérdida de registros o datos -----3
- Revelación de información sensible -----2
- Fallos en el sistema IT -----1

5. ¿A qué servicios o aplicaciones afectaría si el servicio que usted administra deja de funcionar? A todo los servicios pero considerando que el básico esta en el servicio de Admisión.
6. ¿Qué tiempo mínimo considera usted que podría pasar sin la información citada? Máximo un día
7. ¿Quién está a cargo del servicio informático cuando usted está de viaje o en clases? La subdirección de la institución
8. ¿Cómo respalda la información a su cargo y con qué periodicidad lo efectúa? A través de impresiones sin horario definido que se coloca en folder.
9. ¿Dónde guarda la información respaldada? Se guarda en forma jerárquica de metales bajo llave.
10. ¿Qué tipos de seguridad le están configurados a su Servicio? El mismo servicio de alarma e incendio que se aplica en el edificio donde se ubica.
11. ¿Quién tiene acceso a su información? Rectorado, Secretaria y Subdirección.
12. ¿Cómo está protegida la información de su computadora? A través de anti – virus.
13. ¿Qué programas ayudan en la protección de su información?, ¿conoce usted?, ¿cuáles? NOD 32 en su forma elemental.
14. ¿Su computadora o servidor donde está alojado, el servidor tiene backups del hardware? No tiene backups de hardware los implementos tecnológicos están sobre muebles de madera, archivadores metálicos, y gran cantidad de información en papel.
15. ¿Tiene servicio de internet? Si
16. ¿Para qué lo usa frecuentemente? Para consultas académicas, notificaciones del Ministerio de Educación y contacto con los supervisores.
17. ¿En términos económicos, cuál cree que es el monto aproximado que está a su cargo en general en la administración de servicio?

Computadora personal -----	\$ 400,00
Muebles y Enseres -----	\$ 250,00
Útiles de oficina-----	\$ 100,00
Regulador de voltaje -----	\$ 20,00
Archivadores metálicos -----	\$ 400,00
Información impresa y de respaldo -----	\$ 2000,00
TOTAL: -----	\$ 3170,00

Servicio Gestión Humana

Aplicación de Servicio: Office 2007, Adobe Reader versión 9.0, Kerios, Nmap, Snort.

Nombre: Ing. Patricio Martínez B.

Función que desempeña: Representante de Gestión Humana y Analista Técnico.

Años en la Institución: 3 años

Responsabilidades a su cargo:

1. ¿Qué aplicaciones maneja dentro del servicio que usted administra? Los expuestos en la aplicación del servicio con énfasis en el IDS Snort, el control de dominio Kerios y el cuidado a través del firewall Ad – aware
2. ¿Cuál considera usted la información más relevante del servicio que administra? El manejo de archivos correspondientes a aspectos personales de los empleados de la institución según se refieran a asuntos familiares, interpersonales e intrapersonales. Así también lo referente a hojas de vida, experiencia, evaluaciones de las capacitaciones, evaluaciones del desempeño entre otros.
3. Consecuencias de los servicios

Riesgo	Causas	Consecuencias	Probabilidad Ocurrencia	Impacto	Solución
Malware	Dispositivos periféricos	Conflictos de red. Aterrizaje de disco duro Pérdida de información sensible	Mensualmente los conflictos de red y pérdidas de información. Una vez al año los aterrizajes.	No se puede hacer intercambio de información La información sensible no permanece únicamente en el servicio	Mejor capacitación al personal del servicio. Utilización de contraseñas duras.
Sabotaje	Uso de ingeniería social para obtener información	Chantaje. Cambio de contraseñas originales	Continuo por el exceso de personas que ingresan al Servicio	Obtención de servicios personales. Impide el trabajo adecuado del Servicio	Limitar el número de personas que ingresan. Bitácora de las personas atendidas
Robo	Sustracción de imple-	No se puede utilizar adecua-	Continuo por la cantidad de	El trabajo se desarrolla a	Limitar el número de

	mentos tecnológicos	damente los implementos.	gente que ingresa al servicio	medias por que los implementos no trabajan adecuadamente	personas que ingresan. Bitácora de las personas atendidas
Revelación de información sensible.	Aplicación de ingeniería social	Conocimientos de hechos de carácter personal exclusivo.	Bimensual	Pérdida de credibilidad de los empleados	Limitar el número de personas que ingresan. Bitácora de las personas atendidas

4. ¿Cuáles son los riesgos que usted considera que se ve avocado mayoritariamente, en una escala del 1 al 5?

- Incendio -----3
- Tormentas eléctricas ----- 3
- Contaminación y amenazas medio ambientales ----- 2
- Actos de sabotaje -----4
- Robo -----4
- Fallos en el sistema de electricidad -----3
- Fallos en el sistema de comunicación -----3
- Crimen cibernético (malware, hackers, crackers, sniffer, spoofing, etc) -----5
- Pérdida de registros o datos -----3
- Revelación de información sensible -----4
- Fallos en el sistema IT -----3

5. ¿A qué servicios o aplicaciones afectaría si el servicio que usted administra deja de funcionar? Esto implicaría a todos los empleados en general, en consecuencia a todos los servicios.

6. ¿Qué tiempo mínimo considera usted que podría pasar sin la información citada? Máximo un día.

7. ¿Quién está a cargo del servicio informático cuando usted está de viaje o en clases? Msc. Juan Carlos Cobos

8. ¿Cómo respalda la información a su cargo y con qué periodicidad lo efectúa? A través de discos duros externos cada 8 días, particularmente los días sábados cuando existe menor fluctuación de gente

9. ¿Dónde guarda la información respaldada? Disco duro LG
10. ¿Qué tipos de seguridad le están configurados a su Servicio? Servicio de alarma contra incendios y robo. Anti – virus, IDS y Kerios para control de dominios, Nmap para el seguimiento de puertos abiertos que no se han permitido su uso.
11. ¿Quién tiene acceso a su información? Los empleados en esencia de todos los servicios
12. ¿Cómo está protegida la información de su computadora? A través de Anti – virus, IDS como Snort por ser un GNU libre, firewall como ad – aware.
13. ¿Qué programas ayudan en la protección de su información?, ¿conoce usted?, ¿cuáles? Nmap para control de puertos y verificación de manejo de información, Kerios para control de dominios y selección de otorgamiento de servicios.
14. ¿Su computadora o servidor donde está alojado, el servidor tiene backups del hardware? Si se posee backups de hardware a través de la red se almacena la información en el computador principal que actúa como servidor. Las computadoras están ubicadas sobre mesas de tabla aglomerada, pero lastimosamente están sobre alfombra altamente corrosible y de carácter ignífugo. Existen archivadores metálicos y muebles de madera.
15. ¿Tiene servicio de internet? Si
16. ¿Para qué lo usa frecuentemente? Consultas referentes a test, evaluación de capacitación entre otros.
17. ¿En términos económicos, cuál cree que es el monto aproximado que está a su cargo en general en la administración de servicio?

Computadores personales (3 en total) -----	\$ 1350,00
Impresora Samsung laser ML 4010 -----	\$ 80,00
Escáner BenQ 5210 -----	\$ 50,00
Muebles y Enseres -----	\$ 400,00
Útiles de oficina-----	\$ 150,00
Regulador de voltaje -----	\$ 60,00
Archivadores metálicos -----	\$ 800,00
TOTAL: -----	\$ 2890,00

Servicio Auditoría

Aplicación de Servicio: Office 2007, Adobe Reader versión 9.0

Nombre: Lcdo. Pedro Auz

Función que desempeña: Líder auditor ADP

Años en la Institución: 3 años

Responsabilidades a su cargo:

1. ¿Qué aplicaciones maneja dentro del servicio que usted administra? Las especificadas en las aplicaciones de servicio, pero particularmente Excel para llevar a cabo las métricas de auditoría interna de la Institución.
2. ¿Cuál considera usted la información más relevante del servicio que administra? Lo correspondiente a Normas ISO, particularmente a la ISO 9001 – 2008
3. Consecuencia de los servicios

Riesgo	Causas	Consecuencias	Probabilidad Ocurrencia	Impacto	Solución
Revelación de información sensible	Ingeniería social	Mala comparativa entre normas	Dos veces por año	Las normas de la Institución no van acorde con las establecidas en la Norma ISO.	Seleccionar mejor personal de auditoría
Sabotaje	Ingeniería social	Perdida y alteración de datos y archivos.	Dos veces por año	Se altera la información base y el personal no se compromete con el trabajo.	Impedir entregar información sensible a personal no autorizado
Malware	Dispositivos periféricos	Daño eminente a la información relevante	Trimestral	Valores no acordes a lo establecido en la norma	Mejorar la calidad de los anti – virus

4. ¿Cuáles son los riesgos que usted considera que se ve avocado mayoritariamente, en una escala del 1 al 5?

- Incendio -----1
- Tormentas eléctricas ----- 2
- Contaminación y amenazas medio ambientales ----- 2
- Actos de sabotaje -----4
- Robo -----3
- Fallos en el sistema de electricidad -----2
- Fallos en el sistema de comunicación -----1
- Crimen cibernético (malware, hackers, crackers, sniffer, spoofing, etc) -----4
- Pérdida de registros o datos -----4
- Revelación de información sensible -----5
- Fallos en el sistema IT -----3

5. ¿A qué servicios o aplicaciones afectaría si el servicio que usted administra deja de funcionar? Básicamente todo aquello correspondiente a la norma ISO 9001 – 2008, ya que está es el estándar sobre el cual trabajan los Servicios.

6. ¿Qué tiempo mínimo considera usted que podría pasar sin la información citada? Máximo 2 días.

7. ¿Quién está a cargo del servicio informático cuando usted está de viaje o en clases? Lcda. Mariana Collaguazo

8. ¿Cómo respalda la información a su cargo y con qué periodicidad lo efectúa? No se realiza el respaldo, únicamente se mantiene en la computadora de uso o a través de los dispositivos periféricos (flashes principalmente).

9. ¿Dónde guarda la información respaldada? No se guarda la información para ser respaldada.

10. ¿Qué tipos de seguridad le están configurados a su Servicio? Únicamente los dotados por la Curia de la ciudad de Quito ya que ellos son los encargados de cuidar el servicio IT de Auditoría.

11. ¿Quién tiene acceso a su información? Deberían tener únicamente los miembros del equipo auditor, pero también lo conoce la rectoría, vicerrectorado, subdirección ya que el personal de auditoría no es un personal competente en el área.

12. ¿Cómo está protegida la información de su computadora? Como lo señalamos, desconocemos como ya que de ello responde la Curia Diocesana

13. ¿Qué programas ayudan en la protección de su información?, ¿conoce usted?, ¿cuáles?
Por lo expuesto, básicamente lo que conocemos, esto es anti – virus y otros medios con los cuales no estamos familiarizados.

14. ¿Su computadora o servidor donde está alojado, el servidor tiene backups del hardware?
Si posee servidor de backups de hardware el cual se encuentra en las oficinas principales de la Curia. El Servicio de Auditoría se ubica en el laboratorio de contabilidad, por ende estamos sobre piso de madera, cada estación de trabajo se ubica en mesas de madera aglomerada, de última generación, tiene un servidor central el cual posee un programa de control de cada una de las estaciones.

15. ¿Tiene servicio de internet? Si

16. ¿Para qué lo usa frecuentemente? Para uso de los estudiantes, sus trabajos y consultas, para ayuda a los profesores en sus investigaciones y para buscar información pertinente al Servicio de Auditoría como tal.

17. ¿En términos económicos, cuál cree que es el monto aproximado que está a su cargo en general en la administración de servicio?

Servidor DELL Power Edge SC 440 -----	\$ 2500,00
Backups – UPS RS 1200 APC -----	\$ 150,00
Impresora HP Laser P2015 dn -----	\$ 120,00
Kypus Server Appliance -----	\$ 250,00
Router EDIMAX EW 7209 APg -----	\$ 30,00
Estaciones de trabajo Vía Samuel 2 (10 en total)---	\$ 3000,00
Muebles y Enseres -----	\$ 600,00
Útiles de oficina-----	\$ 100,00
TOTAL: -----	\$ 6750,00

14.4. ANEXO 4

14.4.1. Hardware del Servicio de Admisión

TIPO	MODELO CPU/PC	Nº	PROCESADOR	RAM	DISPONIBILIDAD DE DISCO / S.O.
Estación de trabajo	Pentium IV	1	3 GHz	512 MB	60 GB

14.4.2. Software del Servicio de Admisión

SISTEMA	VERSIÓN	PROVEEDOR/SOPORTE	PLATAFORMA	PRINCIPALES CARACTERÍSTICAS	USUARIOS CLAVE
Windows XP	2002	Microsoft Corporation	Intel Pentium	Uso exclusivo del servicio	ADP Auxiliar

14.4.3. Hardware del Servicio de Mantenimiento y Reparaciones (Laboratorio de Computación)

TIPO	MODELO CPU/PC	Nº	PROCESADOR	RAM	DISPONIBILIDAD DE DISCO / S.O.
Estación de trabajo	Pentium Dual Core	PC21	2.51 GHz	1GB	48.8 GB
Estación de trabajo	Pentium Dual Core	PC19	2.51 GHz	1GB	48.8 GB
Estación de trabajo	Pentium 4	PC25	1.60 GHz	224 MB	19 GB
Estación de trabajo	Celeron	PC18	2.54 GHz	224 MB	19 GB
Estación de trabajo	Celeron	PC23	2.54 GHz	224 MB	34.7 GB
Estación de trabajo	Pentium 4	PC19	2.26 GHz	240 MB	18.6 GB
Estación de trabajo	Pentium 4	PC20	2.8 GHz	768 MB	38.1 GB
Estación de trabajo	Dañada	PC22			
Estación de trabajo	Pentium 4	PC26	1.8 GHz	248 MB	19.0 GB
Estación de trabajo	Pentium 4	PC27	1.6 GHz	224 MB	19.0 GB
Estación de trabajo	Dañada	PC28			

trabajo					
Estación de trabajo	Dañada	PC29			
Estación de trabajo	Pentium 4	PC30	2.26 GHz	240 MB	18.5 GB
Estación de trabajo	Pentium 4	PC31	1.6 GHz	224 MB	17.56 GB
Estación de trabajo	Pentium 4	PC32	1.6 GHz	224 MB	19.5 GB
Estación de trabajo	Pentium 4	PC33	1.6 GHz	224 MB	19 GB
Estación de trabajo	Pentium 4	PC37	2.4 GHz	192 MB	18.5 GB
Estación de trabajo	Celeron	PC36	2.54 GHz	244 MB	19 GB
Estación de trabajo	Pentium Dual Core	PC35	2.5 GHz	1 GB	74.5 GB
Estación de trabajo	Celeron	PC34	1.81 GHz	1 GB	74.5 GB
Estación de trabajo	Dañado	PC12			
Estación de trabajo	Dañado	PC24			
Estación de trabajo	Pentium 4	PC17	2.4 GHZ	248 MB	16.6 GB
Estación de trabajo	Pentium Dual Core	Pc23	2.5 GHz	1 GB	48.8 GB

14.4.4. Software del Servicio de Mantenimiento y Reparaciones (Laboratorio de Computación)

SISTEMA	VERSIÓN	PROVEEDOR/SOPORTE	PLATAFORMA	PRINCIPALES CARACTERÍSTICAS	USUARIOS CLAVE	Nº
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	Estudiantes	PC21
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	Estudiantes	PC19
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	Estudiantes	PC25
Windows XP	2002	Microsoft Windows	Intel Celeron	Estación de trabajo	Estudiantes	PC18
Windows XP	2002	Microsoft Windows	Intel Celeron	Estación de trabajo	Estudiantes	PC23
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	Estudiantes	PC

Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	de	Estudiantes	PC20
				Dañada		Estudiantes	PC22
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	de	Estudiantes	PC26
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	de	Estudiantes	PC27
				Dañada			PC28
				Dañada			PC29
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo	de	Estudiantes	PC30
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo		Estudiantes	PC31
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo		Estudiantes	PC32
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo		Estudiantes	PC33
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo		Estudiantes	PC37
Windows XP	2002	Microsoft Windows	Intel Celeron	Estación de trabajo		Estudiantes	PC36
Windows XP	2002	Microsoft Windows	Intel Pentium	Estación de trabajo		Estudiantes	PC35
Windows XP	2002	Microsoft Windows	Intel Celeron	Estación de trabajo		Estudiantes	PC34
				Dañada			PC12
				Dañada			PC24
Windows XP	2002	Microsoft Windows	Intel Pentium	Usuario personal		Profesor	PC23
Windows Server	2003	Microsoft Windows	Intel Pentium	Uso personal		Administrador IT	PC17

14.4.5. Hardware del Servicio de Mantenimiento y Reparaciones (Laboratorio de Contabilidad)

TIPO	MODELO CPU/PC	Nº	PROCESADOR	RAM	DISPONIBILIDAD DE DISCO / S.O.
Estación de trabajo	Intel Pentium	Servidor	2.79 GHz	1 MB	29.2 GB
Estación de trabajo	Intel Celeron	2	1GHz	120 GB	9.75 GB
Estación de trabajo	Intel Celeron	3	2.53 GHz	224 MB	38.3 GB
Estación de trabajo	Intel Pentium	4	2.40 GHz	224 MB	6.03 GB

Estación de trabajo	Intel Pentium	1	2.40 GHz	192 MB	19.0 GB
Estación de trabajo	AMD Duron	9	1 GHz	112 MB	19.5 GB
Estación de trabajo	Intel Pentium		801 GHz	180 MB	3.08 GB

14.4.6. Software del Servicio de Auditoría (Laboratorio de Contabilidad)

SISTEMA	VERSIÓN	PROVEEDOR/SOPORTE	PLATAFORMA	PRINCIPALES CARACTERÍSTICAS	USUARIOS CLAVE	Nº
Windows XP	2002	Microsoft Windows	Intel Pentium	Servidor del Laboratorio		Servidor
Windows XP	2002	Microsoft Windows	Intel Celeron	Uso estudiantes		PC2
Windows XP	2002	Microsoft Windows	Intel Celeron	Uso estudiantes		PC3
Windows XP	2002	Microsoft Windows	Intel Pentium	Uso estudiantes		PC4
Windows XP	2002	Microsoft Windows	AMD Duron	Linux 2 sistemas		PC5
Linux			Operativos			
Windows XP	2002	Microsoft Windows	Intel Pentium 4	Uso estudiantes		PC1

14.4.7. Aplicaciones del Servicio de Auditoría (Laboratorio de Contabilidad)

APLICACIÓN	VERSIÓN	PROVEEDOR/SOPORTE	PLATAFORMA	USUARIOS CLAVE	Nº
Internet Explorer	7.0.6	Microsoft	Windows XP	Docente y estudiante	Servidor
Internet Explorer	6.0.2	Microsoft	Windows XP	Docente y estudiante	PC5
Microsoft Office	2003	Microsoft	Windows XP	Docente y estudiante	
Mónica 7	7	Technotel	Windows XP	Docente y estudiante	PC3
Internet Explorer	6.0.2	Microsoft	Windows XP	Docente y estudiante	PC4
Microsoft Office	2003	Microsoft	Windows XP	Docente y estudiante	
Mónica 7	7	Technotel	Windows XP	Docente y estudiante	

Internet Explorer	6.0.2	Microsoft	Windows XP	Docente y estudiante	PC3
Microsoft Office	2003	Microsoft	Windows XP	Docente y estudiante	
Mónica 7	7	Technotel	Windows XP	Docente y estudiante	
Internet Explorer	6.0.2	Microsoft	Windows XP	Docente y estudiante	PC2
Microsoft Office	2003	Microsoft	Windows XP	Docente y estudiante	
Mónica 7	7	Technotel	Windows XP	Docente y estudiante	
Internet Explorer	6.0.2	Microsoft	Windows XP	Docente y estudiante	PC1
Microsoft Office	2003	Microsoft	Windows XP	Docente y estudiante	
Mónica 7	7	Technotel	Windows XP	Docente y estudiante	
Microsoft Office	2007	Microsoft	Windows XP	Docente y estudiante	
Internet Explorer	6.0.2	Microsoft	Windows XP	Docente y estudiante	PC10
Microsoft Office	2003	Microsoft	Windows XP	Docente y estudiante	

14.5. ANEXO 5

14.5.1. COBERTURA DE DOCENTES Y ESTUDIANTES

Este seguro es proporcionado por Raúl Coka Barriga, la cual nos brinda Seguro sin complicaciones!

COBERTURAS

- Ū Indemnización por muerte accidental
- Ū Desmembración accidental
- Ū Incapacidad total y permanente por accidente
- Ū Perdida de vista oído o voz por accidente
- Ū Gastos médicos por accidente
- Ū Beca estudiantil por muerte accidental del padre o madre o representante económico o falta de los dos
- Ū Beca estudiantil por incapacidad total y permanente por accidente del padre o madre o representante económico o falta de los dos

El presente informativo de seguro, está sujeto a todos los términos, condiciones y exclusiones mencionados en la póliza del seguro. La Compañía de Seguros pagará hasta el límite asegurado, siempre y cuando el asegurado sea alumno regular del plantel educativo.

- De acuerdo al listado proporcionado por la Institución Educativa.

Duplicación del límite del asegurado en caso de accidente si éste ocurre:

Dentro de la Institución Educativa, fuera de la Institución Educativa siempre y cuando se encuentre en representación de la misma. Cuando el estudiante esté siendo transportado en los buses de la Institución Educativa o contratados por la misma.

(No aplica en Plan Educación Segura, Beca Estudiantil ni Renta Diaria por Hospitalización)

¿Cómo funciona el SOAT?

En un accidente de tránsito, la persona herida (peatón, conductor, acompañante) debe acudir a ser trasladado al hospital o clínica más cercano y solicitar la atención médica pertinente. Los profesionales médicos, así como las clínicas u hospitales públicos y privados autorizados están obligados a prestar sus servicios hasta \$ 2.500,00 USD por persona.

El seguro Raúl Coka Barriga, aplicara una vez superados los \$ 2.500,00 USD.

Cobertura en cualquier parte del mundo, 24 horas al día, 365 días del año.

- Información 24 horas del día, 365 días del año.
- Orientación medica telefónica.
- Auxilio médico con ambulancia a nivel nacional e internacional.

- Crédito hospitalario por accidente en emergencia.
- Pago inteligente reembolso de reclamos en 24 horas.
- Asistencia en viajes nacionales e internacionales, traslado o repatriación de restos mortales.
- Asistencia exequial por muerte accidental.
- Consultas medicas ilimitadas desde \$6,99.
- Plan dental primera consulta gratis, 20% descuento en tratamiento.

Este seguro consta con el respaldo de: EQUIVIDA Seguros para Personas

PROCEDIMIENTOS:

En caso de emergencia y hospitalización por accidente:

1. Comunicarse con Asistencia total RAUL COKA BARRIGA al 1800-raul coka (1800-728-526) o al 099-911-911 las 24 horas del día, los 365 días el año y desde cualquier lugar del mundo. Desde el exterior marca 593(2)2 990 778.
2. Trasladarse inmediatamente al hospital en convenio más cercano.
3. Presentar la tarjeta de RAUL COKA BARRIGA
4. Presentar la cédula carné estudiantil o documento de identificación.
5. Completar y firmar el formulario de reclamación que será entregado en el hospital.
6. Cancelar el deducible correspondiente.
7. Si la cuenta del hospital excede el límite para gastos médicos, deberá cancelar la diferencia.
8. Entregar una garantía en caso de hospitalización, cirugías o cuando la cuenta del hospital supere los \$ 1.000.

Pago de reclamos vía reembolso en caso de accidente

1. Comunicarse con Asistencia total RAUL COKA BARRIGA al 1800-raul coka (1800-728-526) o al 099-911-911 las 24 horas del día, los 365 días el año y desde cualquier lugar del mundo. Desde el exterior marca 593-2-299-0778.
2. Informar nombre del asegurado, fechas y circunstancias del accidente.
3. Solicitar a las oficinas de RAUL COKA BARRIGA el formulario de reclamación o descargarlo de: <http://www.raulcoka.com/colegios/2E/rcb.html>
4. Completar el formulario de reclamación, firmado y sellado por el médico tratante y entregarlo en nuestras oficinas con los siguientes documentos:
 - Facturas de todos los gastos incurridos con desglose y debidamente firmadas
 - Recetas y órdenes médicas
 - Resultados de exámenes y radiografías
 - Copias de Hoja de Atención de Emergencia y/o Historia Clínica

Las facturas deben ser representadas en originales y cumplir con el reglamento de facturación.

IMPORTANTE: La notificación del accidente debe realizarse dentro de los 60 días contados a partir de ocurrencia del mismo, caso contrario quedará extemporáneo.

14.6. ANEXO 6

14.6.1. BOTIQUIN DE PRIMEROS AUXILIOS

MEDICACIÓN	CANTIDAD
Solución salina al 0,9%	1
Guantes quirúrgicos	1
Diclofenaco gel	1
Cicatrex crema	1
Garamicina crema	1
Equipo de venoclisis	1
Introcar	1
Jeringa de 3 cc.	2
Jeringa de 5 cc.	1
Vendas de gasa	2
Visina	1
Sablón	1
Suero fisiológico	1
Violeta de genciana	1
Sedas 3/0	1
Paracetamol tabletas	10
Paracetamol jarabe	1
Gasas	1
Jelonet	1
Torundas	1
Alcohol	1
Tijera	1
Pinza	1
Esparadrapo cinta	1

Glosario

- **ADP:** Administrador del Proceso, del Servicio en el presente proyecto.
- **BIA:** Análisis de Impacto en el Negocio
- **BRT:** Equipo de Recuperación del Negocio
- **CID:** Confidencialidad, Integridad y Disponibilidad
- **CNT:** Consejo Nacional de Telecomunicaciones
- **COBIT:** Objetivo de Control para la Tecnología de la Información
- **DRP:** Plan de Recuperación de Desastres.
- **DRT:** Equipo de Recuperación del Desastre
- **EMSAT:** Empresa Metropolitana de Servicio y Administración del Transporte
- **Extintores tipo ABC:** **A** = madera, papel, telas de algodón, etc., **B** = pintura, gasolina, solventes, etc., **C** = conectores electrónicos.
- **GHz:** Gigahertz
- **GNU:** del inglés “ñu”, acrónimo de GNU no es Unix.
- **IDS:** Sistema Detector de Intrusos
- **ISO:** Organización Internacional de Estándares
- **IT:** Tecnología de la Información
- **PCI:** Plan Curricular Institucional
- **PCN:** Plan de Continuidad de Negocios
- **PEI:** Proyecto Educativo Institucional
- **PUD:** Plan de Unidad Didáctica
- **RJ:** Registered Jack
- **SPM:** Steganos Password Manager
- **UPS:** Sistema de Energía Ininterrumpible
- **WEB:** Telaraña
- **XP:** Experiencia

Bibliografía

1. CEPEDA, F (2008, mayo): Plan de Continuidad de Negocio (en línea). México D.F. Disponible en WWW: <http://www.seguridaddescifrada.blogspot.com>
2. BALLESTER, M (2005, septiembre): Continuidad de Negocio (en línea). Madrid. Disponible en WWW: <http://www.firstconference.org>
3. PONCE, P (2008, abril): Seguridad de la Información (en línea). Nuevo México. Disponible en WWW: <http://www.santafeassociates.com>
4. PEÑA IBARRA, J (2004,): Planes de Contingencia, Recuperación de Desastres (en línea). México D.F. Disponible en WWW: <http://www.ccisa.com.mx>
5. CARDENAS, D (2004): Planificación de la Continuidad del Negocio: Estar preparados para lo que pase (en línea). Disponible en WWW: <http://www.kpmg.com.mx>
6. BORGHELLO, C (2001, septiembre): Seguridad Informática: sus implicancias e implementación (en línea). Buenos Aires. Disponible en WWW: <http://www.segu-info.com.ar/tesis/>
7. BORGHELLO, C (2001, septiembre): Seguridad Informática: políticas de seguridad (en línea). Buenos Aires. Disponible en WWW: <http://www.segu-info.com.ar/politicas/>
8. ARGENTERO, C (2006, septiembre): ISO 17799 La Seguridad Informática no es un producto sino un proceso (en línea). Córdoba. Disponible en WWW: <http://www.deobit.com>
9. VeriSign iDefense Security Intelligence Service (2009) (en línea) Madrid, Es.: VeriSign, (citado 12 diciembre 2009). Disponible en Internet: < <http://www.verisign.es/security-intelligence-service/index.html> > Mensual
10. Seguridad Informática: ¿qué, porqué y para qué? (2002) (en línea) México D.F. Mx.: CyberHabitat ciudad de la informática, (citado 5 noviembre 2009). Disponible en Internet: <http://ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm>
11. Servicios – Consultoría (2010) (en línea) Barcelona, Es.: E.Zone solutions, (citado 7 enero 2010). Disponible en Internet: < <http://www.ezone.net/es/servicios/soluciones-de-continuidad> >
12. La guía fundamental para la recuperación de desastres: cómo garantizar la continuidad en equipos informáticos y actividades comerciales (2008) (en línea). California, Eu.: Vision Solutions. Disponible en WWW: <http://visionsolutions.com>
13. ANTON, F. (2007) “El objetivo es proporcionar mecanismos de reacción ante posibles interrupciones de los servicios para proteger los procesos considerados críticos”. PLAN DE CONTINUIDAD DE NEGOCIOS, Rev. De Perspectiva Empresarial. 92 – 95.
14. ALVAREZ, G., PEREZ P. (2004): Seguridad Informática para empresas y particulares. Madrid: Ed. McGraw Hill.

15. PIATTINI M., DEL PESO E. (2001): Auditoría Informática, un enfoque práctico. México D.F: Ed. Alfaomega – RAMA.
16. CARVAJAL I. (2001): Jurismática, conceptos indispensables. Quito: Ed. Diagramación: Tinta & Papel.
17. CONNOLLY THOMA M. (2007): Sistema de Bases de Datos, un enfoque práctico para diseño, implementación y gestión. Madrid: Ed. Pearson – Addison Wesley.
18. KOONTZ H., WEHRICH H. (2005): Administración, una perspectiva global. México D.F.: Ed. McGraw Hill.
19. WHITTINGTON R., KURT P. (2006): Principios de Auditoría. México D.F.: Ed. McGraw Hill.
20. SILBERSCHATZ A., GALVIN P. (2003): Sistemas Operativos. México D.F.: Ed. Addison – Wesley.
21. CHAMOUN Y. (2007): Administración Profesional de Proyectos. México D.F.: Ed. McGraw Hill.