EMMSA
Empresa Municipal
de Mercados S.A.

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD"

RESOLUCIÓN DE GERENCIA GENERAL No. 016-GG-EMMSA-2019

Santa Anita, 29 de Marzo de 2019

VISTO:

El Informe No. 012-2019-GAF-EMMSA de la Gerencia de Administración y Finanzas, y el Informe No. 002-SGI-EMMSA-2019 de la Sub Gerencia de Informática; y,

CONSIDERANDO:

Que, la Empresa Municipal de Mercados SA - EMMSA es una Empresa Municipal de derecho privado, organizada bajo la forma de Sociedad Anónima, que goza de autonomía técnica y administrativa; siendo sus acciones y patrimonio de total propiedad de la Municipalidad Metropolitana de Lima. Se rige por sus estatutos, por las disposiciones que le sean aplicables de la Ley No. 27972, Ley Orgánica de Municipalidades, sin perjuicio de las disposiciones que regulan el Sistema Nacional de Control.

Que mediante Resolución Ministerial No. 019-2011-PCM, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) aprobó la Guía para la elaborar la Formulación y Evaluación del Plan Operativo Informático (POI) de las Entidades Administración Pública;

Que el Plan Operativo Informático (POI) constituye un instrumento de gestión que permite definir, priorizar, evaluar y orientar las actividades informáticas de las Entidades de la Administración Pública, teniendo como objeto la creación de una estructura informática y de servicios que permita el cumplimiento de los objetivos institucionales;

Que mediante Resolución Ministerial No. 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Sistema de Gestión de la Seguridad de la Información", la cual dispone la elaboración del Plan de contingencia cuya finalidad es implementar las buenas prácticas para la gestión de la seguridad de la información.

Que el Plan de contingencia constituye un instrumento para la aplicación obligatoria ante las contingencias de tipo informático que ocurran en la Entidad.

Que mediante Informe No. 001- SGI-EMMSA-2019. La Subgerencia de Informática sustenta la necesidad de aprobar el Plan Operativo Informático 2019, y el Plan de Contingencia Informático 2019 de EMMSA, con la finalidad de la creación de una estructura informática y de servicios que permita el cumplimiento de los objetivos institucionales y la aplicación obligatoria de las contingencias de tipo informático que ocurran en la entidad

Que la Gerencia de administración y Finanzas de EMMSA con Memorando No. 012-2019-GAF-EMMSA ha presentado para su aprobación el Plan Operativo Informático 2019, y el Plan de Contingencia Informático 2019 de EMMSA,

De conformidad a las facultades conferidas a la Gerencia General, con las visaciones de la Gerencia de Administración y Finanzas, la Gerencia de Planeamiento Presupuesto y Estadística, de la Gerencia de Asesoría Legal y la Subgerencia de Informática.

GERENCIA GENERAL V°B° J. GALLEGOS R. GERENTE EMMSA

GERENCIA DE ASESORIA LEGAL V°B° A. REYES GERENTE EMMSA

GERENCIA DE PLANEAMIENTO, PRESUPUESTO Y ESTADISTICA V°B° L. CASTILLO GERENTE(e) EMMSA

GERENCIA DE ADMINISTRACION Y FINANZAS V°B° M.GARCIA EMMSA

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD"

SE RESUELVE:

ARTÍCULO PRIMERO.- Aprobar el "Plan Operativo Informático 2019" de la Empresa Municipal de Mercados Sociedad Anónima - EMMSA, cuyo texto en anexo forma parte integrante de la presente Resolución.

ARTÍCULO SEGUNDO.- Aprobar el "Plan de Contingencia Informático 2019" de la Empresa Municipal de Mercados Sociedad Anónima - EMMSA, cuyo texto en anexo forma parte integrante de la presente Resolución.

ARTÍCULO TERCERO.- Disponer que el cumplimiento del Plan Operativo Informático 2019" y del "Plan de Contingencia Informático 2019", será responsabilidad de la Subgerencia de Informática de la entidad.

ARTÍCULO CUARTO.- Encargar a la Subgerencia de Informática efectuar el seguimiento y evaluación del cumplimiento de los Planes que por la presente resolución se aprueba.

ARTÍCULO QUINTO.- Disponer la publicación del "Plan Operativo Informático 2019" y del "Plan de Contingencia Informático 2019" en el Portal Institucional, y en el Portal del Estado Peruano, en el plazo de un (1) día de su aprobación, de conformidad con lo establecido en el artículo 3º de la Ley No. 29091.

Regístrese, Comuníquese y Cúmplase.

EMPRESA MUNICIPAL DE MERCADOS S.A.
JAIME ADHEMIR GALLEGOS RONDON
GERENTE GENERAL

MUNICIPALIDAD DE LIMA

EMMSA
Empresa Municipal de Mercados S.A.

Plan Operativo Informático 2019

Resolución de Gerencia General No. 016-2019-GG-EMMSA

www.munlima.gob.pe

MUNICIPALIDAD DE LIMA

1. Misión de la Dirección o Gerencia Informática

La Subgerencia de Informática tiene como misión promover el desarrollo informático integral de EMMSA, con el fin de optimizar los procesos de información para mejorar la toma de decisiones, con propuestas innovadoras integradoras y modernas, contribuyendo a la mejora continua de calidad y con la adecuada prestación del servicio a nuestros usuarios directos e indirectos, de forma eficiente.

2. Visión de la Dirección o Gerencia Informática

Ser una Subgerencia líder en producción de soluciones tecnológicas que satisfagan adecuadamente los requerimientos de las diferentes áreas de la empresa a través de servicios oportunos y de alta calidad.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

3. Análisis Situacional de la Oficina de Informática

Con la finalidad de adoptar medidas orientadas a la modernización de EMMSA, se ha realizado el análisis y diagnóstico situacional de la oficina de informática, el cual detallamos a continuación:

3.1 Recursos Humanos

La Sub Gerencia de Informática está compuesta por siete (08) colaboradores, los cuales se detallan en la Tabla No. 01:

EMMSA
Empresa Municipal de Mercados S.A.

CARGO / FUNCIÓN	CANTIDAD
Sub Gerente de Informática	1
Asistente Administrativo	1
Desarrollo de Sistemas	
Especialista	2
Administrador de Redes	2
Desarrollador Web	1
Practicante	
Soporte Técnico	1
TOTAL	**8**

Tabla No. 01: Personal Asignado a la Sub Gerencia de Informática

4. Situación Actual - Localización y Dependencia Estructural y/o Funcional

La Subgerencia de Informática es un órgano de apoyo a la gestión de la Gerencia de Administración y Finanzas de quien depende directamente.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

5. Situación Actual - Recursos Tecnológicos e Informáticos existentes:

5.1. Hardware

ITEM	MARCA	MODELO	HDD	RAM	PROCESADOR	CANTIDAD	GARANTIA
1	HP	Compaq Elite 8300	239	4	Ci5	1	NO
2			265	4	Ci5	1	NO
3			460	4	Ci5	1	NO
4			462	4	Ci5	1	NO
5			465	4	Ci5	37	NO
6			465	4	Ci5	1	3 años
7			465	8	Ci5	1	NO
8			470	4	Ci5	8	NO
9			809	8	Ci7	1	NO
10			1 TB	8	Ci5	2	NO
11		Compac DC 5700	127	2	Core2Duo	1	NO
12		Compac DC 5700	230	2	Core2Duo	1	NO
13			232	2	Core2Duo	2	NO
14			292	2	Core2Duo	1	NO
15			298	2	Core2Duo	1	NO
16			232	2	Ci5	1	NO
17		Compaq Elite 8200	456	4	Ci7	1	NO
18		ELITEDESK 800 G3 SFF	1TB	16	Ci5	1	NO
19		HP PRO 3000MT	320	2	Ci5	1	NO
20			269	3	Ci5	1	NO
21		Omni 27pc	1042	8	Ci5	1	NO
22	DELL	Optiplex 7050	1TB	8	Ci7	7	3 años
23		Optiplex 790	450	4	Ci5	2	NO
24			451	4	Ci5	1	NO
25			452	4	Ci5	9	NO
26			455	4	Ci7	2	NO
27			455	4	Core2Duo	1	NO
28			460	4	Ci5	2	NO
29			465	4	Ci5	5	NO
30		Optiplex 9020	470	4	Ci5	1	NO
31			465	4	Ci7	1	NO
32			465	4	Ci7	1	NO
33			1TB	8	Ci7	16	NO
34			1TB	8	Ci7	1	NO
35			1TB	16	Ci5	1	NO
36			1TB	4	Ci7	7	3 años
37	LENOVO	ThinkCentre	465	4	Core2Duo	1	NO
38			465	4	Ci5	1	NO
39	PC Compatible	Pc compatible	500	3	Core2Duo	1	NO

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

5.2. Equipos Portátiles.

EMMSA cuenta con un total de nueve (09) equipos portátiles. Es importante mencionar que de estos equipos, cinco (05) se encuentran en proceso de baja y los cuatro (04) restantes no cuentan con Garantía. La relación de portátiles se detalla en la Tabla No. 03.

Tabla No. 03: Equipos Portátiles

ITEM	MARCA	MODELO	HDD	MEM (MB)	PROCESADOR	CANTIDAD	GARANTÍA
1	TOSHIBA	PORTEGE R-930-SP33462	285	4	Ci5	1	NO
2		PORTEGE Z835 - SP3241L	130	6	Ci5	1	NO
3		SATELLITE C845 - SP4334SL	455	4	Ci3	2	NO
4		SATELLITE C845 - SP4334SL	455	4	Ci3	1	BAJA
5		TECRA A10 - SP5801	265	3	CORE 2DUO	1	BAJA
6		TECRA A10 - SP5801	300	4	Ci5	1	BAJA
7	DELL	LATITUDE E5520	284	4	Ci5	3	NO
8		LATITUDE E5520	284	4	Ci5	1	BAJA
9	HP	COMPAQ 6710b	147	2	CORE 2DUO	1	BAJA

e

Fuente: Elaboración Propia – EMMSA 2019

5.3. Impresoras

EMMSA cuenta con un total de treinta y seis (36) impresoras, las cuales a la fecha no cuentan con Garantía. La relación de impresoras se detalla en la Tabla No. 04.

Tabla No. 04: Impresoras

ITEM	MARCA	MODELO	TIPO DE IMPRESORA					CANTIDAD	GARANTIA
			MULTI FUNCIONAL	LASER	MATRICIAL	TERMICA	TIQUETERA		
1	EPSON	DFX-9000			x			1	NO
2		FX-2190			x			2	NO
3		L455	x					1	NO
4		LQ-2090			x			3	NO
5		LX-300+II			x			3	NO
6		M244A				x		1	NO
7	HP	LASERJET 1160		x				1	NO
8		LASERJET 1300		x				1	NO
9		LASERJET 500 COLOR MS51		x				1	NO
10		LASERJET 5200FN		x				1	NO
11		LASERJET M1212NF MFP	x					10	NO
12		LASERJET P2035N		x				1	NO
13		LASERJET P3005N		x				1	NO
14		LASERJET P2055DN		x				1	NO
15		LASERJET P3015		x				3	NO
16		LASERJET CP1515N		x				1	NO
17		OFFICEJET 6000	x					1	NO
18		M1522NF		x				1	NO
19	KONICA MINOLTA	554E	x					1	NO
20		BIZHUB 215	x					1	NO
21		BIZHUB 363	x					6	NO
22		BIZHUB 367	x					1	NO
23		BIZHUB 554E	x					2	NO
25		BIZHUB 215	x					3	NO
26	PLOTTER HP	DESINGNJET 111		x				1	NO
27	SAMSUNG	PROXPRESS M4508FX	x					2	NO
28	STAR	BSC10UC				x		12	NO
29		SP700R					x	5	NO
30		SP700R			x			2	NO
31	XEROX	PHASER 6280		x				2	NO

Fuente: Elaboración Propia – EMMSA 2019

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

5.4. Estabilizadores

EMMSA cuenta con un total de veintiséis (26) estabilizadores, las cuales a la fecha no cuentan con Garantía. La relación de estabilizadores se detalla en la Tabla No. 05.

Tabla No. 05: Relación de Estabilizadores

ITEM	MARCA	MODELO	CANTIDAD	GARANTÌA
1	CDP	B-AVR1006	1	NO
2	DINA POWER	SOLIDO 1000	4	NO
3	ELISE	EATON DX2000H	1	NO
4	FES	FES10	1	NO
5	GPD	BY PASS	1	NO
6	HEVYS ENGINERING	S/N	13	NO
7	ICOM POWER	SPC – 2145HL	1	NO
8	MEGA	PCG1200	7	NO
9	MINI – POWER	SOLIDO 1000	1	NO
10	OMEGA	S/N	1	NO
11	POWER SAFE	LCR – 15	67	NO
12	POWER SERVICE	EST – 2012 – 0209	1	NO
13		EST – 2012 – 0227	1	NO
14		EST – 2012 – 0227	1	NO
15		EST – 2012 – 0231	1	NO
16		EST – 2012 – 0232	1	NO
17		EST – 2012 – 0238	1	NO
18		EST – 2012 – 0243	1	NO
19		EST – 2012 – 0233	1	NO
20		EST – 2012 – 0246	2	NO
21		EST – 2012 – 0248	1	NO
22	SUPER TRONY	DHL	1	NO
23	SUPER - APC	BACK - UPS	4	NO

Fuente: Elaboración Propia – EMMSA 2019

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMÍREZ SUB-GERENTE EMMSA

5.5. Servidores

En la Tabla No. 06, se detalla la relación de servidores con que cuenta EMMSA. Es importante mencionar que los bienes en mención solo la de Servidores de Archivos y de Base de Datos tienen garantía por 3 años.

Tabla No. 06: Relación de Servidores

SERVIDORES DEL MERCADO MAYORISTA DE LIMA												
	FUNCION	SERVIDOR DE ARCHIVOS	SERVIDOR DE BASE DE DATOS	SERVIDOR DE TRÁMITE DOCUMENTARIO	SERVIDOR MARCADOR DE PERSONAL	SERVIDOR WEB	SERVIDOR DETECTOR DE PLACAS	SERVIDOR BACKUP	SERVIDOR ANTIVIRUS	HNVR1	HNVR2	HNVR3
	HOSTNAME	ORAEMMSA	EMMSADB	GESDOC	CC-TLC-SRV03	WEBSERVER	DETECTOR	BACKUP		CAMARAS	CAMARAS	CAMARAS
	APLICACIONES	Archivos, Documentos, etc.										
CARACTERISTICAS	SISTEMA OPERATIVO	Windows Server 2016 Standard	W.Server 2016	LINUX CENTOS	W.SERVER 2008	W.2012	W10	W.Server 2003 R2				
	MARCA	HP	HP	DELL	DELL		GENETEC	DELL	HP			
	MODELO	PowerEdge R440	ProLiant DL360 Gen10	Power Edge R620	Power Edge R620	Proliant DL 360e Gen8	STREAMVAULT	Power Edge R710	PRO300MT			
	DISCO DURO		4 TB		700gb	600 GB		700gb	250 GB			
	MEMORIA RAM		32gb		32gb	10 GB		4gb	2 GB			
	PROCESADOR	Intel Xeon 4114	Intel Xeon Silver4114 2.2 GhZ		intel xeon e5-2650 2.0 GhZ	INTEL XEON e5-2403 1.80GhZ	INTEL CORE I3	INTEL XEON 5520 2.27GhZ				
	SERIE	GXG6RP2	MXQ74301PN	H52QDV1	8R2QDV1	MXQ31800BQ	120201002UA7481V7M	JHBWVH1	MXL01002S3			
	INVENTARIO	7408920000007	7408920000006	74089200000005	74089200000004	74089200000002	95224565000002		74089950000017			
	IP	10.00.0.4		10.00.0.0	10.00.0.5	10.70.0.104 10.70.0.40	10.30.0.120	10.00.0.0	10.00.0.10			
	ESTADO	Operativo										
	GARANTÍA	03 Años	03 Años									

Fuente: Elaboración Propia – EMMSA 2019

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

5.6. Otros

Anexos Telefónicos	83
Central Telefónica	1
PDA	1
Proyector Multimedia	2

5.6.1 Software

Nº	SOFTWARE	CANTIDAD
Sistemas Operativos		
1	Windows 7 Profesional 32 bits	0
2	Windows 7 Profesional 64 bits	110
3	Windows 8 Profesional 64 bits	16
4	Windows Server 2003 STD	2
5	Windows Server 2008	1
6	Windows Server 2012	2
7	Windows Vista	1
8	Windows Xp Professional	8
9	Windows 10	36
Motores de Base de Datos		
10	Oracle 11G	1
Herramientas de Desarrollo		
11	Team Developer GUPTA	1
12	Visual Fox Pro 2013	3
13	Visual Fox Pro 6 (32 bits)	5
De Oficina		
14	Microsoft Office 2010	116
15	Microsoft Office 2013	5
16	Sistema de Marcación Electrónica	2
17	Office 2016	11
18	Office 2019	14
Antivirus		
19	Eset NOD32	200
Otros		
20	Adobe Acrobat STD 8.0	1
21	Autocad 2020	4
22	S10 2018	4
23	Sistema Peruano de Informacion Juridica (SPIJ)	5
24	Winzip 8.0	6
25	Adobe Creative Cloud Premiun	1

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

5.6.2. Conectividad

Nº	CONECTIVIDAD	CANTIDAD
Switches		
1	Switch 16 Puertos	1
2	Switch 24 Puertos	11
3	Switch 48 Puertos	6
4	Switch 8 Puertos	4
5	Switch Core	1
Wireless		
6	Acces Point	10

SUB-GERENCIA DE INFORMÁTICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

6. Situación Actual - Problemática Actual

6.1. Debilidades

Nº	LISTADO DE DEBILIDADES
01	No se cuenta con un centro de cómputo alterno para casos de desastre o contingencia.
02	El Portal web de la empresa no es bien aprovechado como herramienta de comunicación con otras empresas privadas y públicas, o como medio de colaboración con los comerciantes.
03	Falta de equipamiento para respaldo total del sistema de video vigilancia.
04	Carencia de un Plan de Capacitación al personal especializado
05	Carencia de un plan de Capacitación a los usuarios en el uso eficientemente de los recursos tecnológicos de EMMSA.
06	Sistema de información desarrollada en una plataforma obsoleta

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

7. Situación Actual - Problemática Actual

7.1. Fortalezas

Nº	LISTADO DE FORTALEZAS
01	Grupo Electrógeno y UPS de media capacidad, para la continuidad del trabajo (garitas y sala de servidores). En caso de ausencia de fluido eléctrico.
02	Se cuenta con un sistema cliente servidor para el registro y administración de la marcación del control del personal de la empresa.
03	Correo Institucional con tecnología y buenas prácticas de seguridad que se ejecutan en la nube, ahorrando un alto costo en infraestructura para este servicio.
04	Sistema integrado de gestión que es de ayuda para la toma de decisiones.
05	Se cuenta con un motor de base de datos reconocido en el mercado.
06	Servicio de custodia para el respaldo externo de las copias de seguridad de información de la empresa.
07	Programas fuentes de los principales sistemas de la institución incluyendo el de la página web.
08	Se cuenta con un firewall corporativo protegiendo y restringiendo los accesos externos a la red de EMMSA, protección contra amenazas, sistema de prevención de intrusos, filtrado web y antispam.
09	Software antivirus para el total de equipos de cómputo e inclusive a los servidores de la empresa a fin de garantizar la seguridad en el acceso a los datos que se procesan en cada uno de ellos.

SUB-GERENCIA DE INFORMÁTICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

8. Situación Actual - Problemática Actual

8.1. Amenazas

Nº	LISTADO DE AMENAZAS
01	Posibilidad de fuga de información de importancia, ya que no se ha implementado un sistema de seguridad de la información en la organización.
02	Cambios en las normativas del estado de índole tecnológico que requieran apoyo de la alta dirección para su implementación.
03	El no cumplimiento de manera responsable por parte de los usuarios de las Normas, Directivas y Resoluciones Informáticas.
04	Posibles ataques informáticos sobre los servidores de la red
05	corporativa.
	Debilidad en el sistema de energía eléctrica, afectando la continuidad de los procesos de gestión y servicios informáticos

SUB-GERENCIA DE INFORMÁTICA
V°B°
I. RAMÍREZ
SUB-GERENTE
EMMSA

9. Situación Actual - Problemática Actual

9.1. Oportunidades

Nº	LISTADO DE OPORTUNIDADES
01	Desarrollo e Implementación de un nuevo Sistema integrado de Gestión.
02	Implementación de Normas ISO9001, ISO14001, ISO27001, ISO 37001
03	Implementación del Sistema de Gestión Documental (Cero papel – Microformas Digitales – Interoperabilidad – Aplicativo de Firma Digital)
04	Implementación y Mejora en el portal web de EMMSA para que sea aprovechado como herramienta de comunicación con la ley de las personas con discapacidad. Ley n° 29973. Y como medio de colaboración con los comerciantes.
05	Implementación de transmisión online de las subastas por medio de la página web Institucional, y redes sociales.
06	Mejora continua de los procesos y procedimientos orientados a brindar un mejor servicio a los usuarios internos y/o externos de la empresa
07	Implementación de modelos de gestión como ITIL, COBIT, CMMI y otros que apoyan en la implementación de buenas prácticas para la gestión de la infraestructura tecnológica.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

10. Alineamiento con el Plan Estratégico Institucional y Sectorial - Objetivos Sectoriales

Nº	LISTADO DE OBJETIVOS
01	Optimizar la calidad de información estadística de productos agrícolas generada en el GMML y que será utilizada por los agentes intervinientes, promoviendo de esa manera un mejor desarrollo en el abastecimiento y comercialización de los productos agrícolas en el Departamento de Lima.
02	Automatizar los procesos de EMMSA y que generan información oportuna para un mejor análisis en la comercialización de productos agrícolas.
03	Proponer soluciones tecnológicas al Gran Mercado Mayorista de Santa Anita para que este mejore la comercialización de productos agrícolas.

SUB-GERENCIA DE INFORMÁTICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

11. Alineamiento con el Plan Estratégico Institucional y Sectorial - Objetivos Institucionales

Nº	LISTADO DE OBJETIVOS
01	Proponer el desarrollo de nuevos sistemas informáticos que automaticen los procesos manuales e integre la información de la empresa.
02	Proponer soluciones tecnológicas que apoyen al desarrollo y ampliación del nuevo Gran Mercado Mayorista de Lima.
03	Administrar eficientemente los recursos tecnológicos de EMMSA para el logro de sus objetivos internos.
04	Mejorar las funcionalidades de las diversas Subgerencias para el logro de la mejora de los procesos Institucionales.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

12. Alineamiento con el Plan Estratégico Institucional y Sectorial - Objetivos Específicos

Nº	LISTADO DE OBJETIVOS
01	Definir las políticas de seguridad, procedimientos y planes de contingencia que garanticen el procesamiento adecuado de información en EMMSA.
02	Garantizar una eficiente arquitectura de red y equipamiento adecuado que permita el desarrollo de las labores de las diversas áreas de EMMSA.
03	Implementar y fomentar programas de capacitación a los usuarios que hagan uso de forma eficiente de los recursos tecnológicos de EMMSA.
04	Contribuir a mejorar el acceso a la Información de los servicios de la empresa, a través de la publicación en el Portal web institucional para todo los usuarios incluyendo a los usuarios con alguna discapacidad.
05	Brindar soporte informático a todas las áreas de EMMSA para el desarrollo de sus actividades.
06	Promover la investigación de nuevas tecnologías para su aplicación en la institución con la finalidad de brindar un mejor servicio a nuestros usuarios.

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMÍREZ SUB-GERENTE EMMSA

13. Estrategias para el logro de las metas del Plan Operativo Informático

13.1. Estrategias

Nº	LISTADO DE ESTRATEGIAS
01	Programar las actividades con las áreas usuarias priorizando el cumplimiento del objetivo institucional.
02	Involucrar al personal de la empresa ante la importancia de la tecnología, para el cumplimiento de sus metas.
03	Administrar de manera eficaz los recursos informáticos con los que cuenta la empresa para cubrir las necesidades informáticas de la institución.
04	Distribuir de acuerdo al perfil profesional de los miembros de la oficina las labores para su pronta ejecución.

SUB-GERENCIA DE INFORMÁTICA
V°B°
I. RAMÍREZ
SUB-GERENTE
EMMSA

14. Programación de Actividades y/o Proyectos Informáticos

I. Denominación de la actividad o proyecto **Orden** **03**

Mantenimiento de Sistemas de Información.

Descripción del proyecto:

La Subgerencia de Informática cuenta con los programas fuentes de los distintos sistemas de información, el mantenimiento periódico es de acuerdo a requerimiento de los usuarios o para su optimización.

TIPO:

Actividad

TIPO DE ORIENTACION:

Orientado a la Gestión Interna

Prioridad:

1

II. Datos Generales

2.1 Unidad Ejecutora:

EMMSA

2.2 Duración9

Fec. Inicio 02/01/2019 Fec. Fin 28/12/2019

2.3 Costo Total:

90000

III. Del proyecto

3.1 Descripción de la Actividad/proyecto:

Análisis y desarrollo de nuevas aplicaciones y opciones de los sistemas. Adecuaciones y modificaciones a los módulos de los sistemas. Optimización de procesos y aplicativos informáticos. Pruebas y puesta en marcha.

3.2 Objetivos de la actividad/proyecto:

Contar con sistemas de información aplicados a la necesidad de la empresa con personal de EMMSA

IV. Meta Anual

100

V. Cobertura de Acción

Institucional

VI. Instituciones Involucradas

EMMSA

VII. Productos Finales

SAFIM / Trámite Documentario

VIII. Usuarios de Productos Finales

200

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Usuarios:

Número de Usuarios Beneficiados	200	Número de Usuarios que demandan	200

I. Denominación de la actividad o proyecto **Orden** **05**

Desarrollo y Mejoramiento de la Página Web Institucional

Descripción del proyecto:

Optimizar la Pagina Web Institucional de EMMSA para estar acorde de la norma aprobada para el CONADIS respecto a las visualizaciones de opciones que permitan el acceso para el manejo de la página web para personas con discapacidad.

TIPO:

Actividad

TIPO DE ORIENTACION:

Orientado a la Gestión Interna

Prioridad:

1

II. Datos Generales

2.1 Unidad Ejecutora:

EMMSA

2.2 Duración:

Fec. Inicio 01/11/2019 Fec. Fin 30/11/2019

2.3 Costo Total:

10,000

III. Del proyecto

3.1 Descripción de la Actividad/proyecto:

Nuevos accesos y mejoras de la página web de EMMSA para las personas con discapacidad.

3.2 Objetivos de la actividad/proyecto:

Contar con una página accesible para todos los tipos de usuario y dar la facilidad para los usuarios con discapacidad.

IV. Meta Anual

100

V. Cobertura de Acción

Institucional

VI. Instituciones Involucradas

EMMSA

VII. Productos Finales

Página Web de EMMSA www.emmsa.com.pe

VIII. Usuarios de Productos Finales

1000

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Usuarios:

Número de Usuarios Beneficiados	1000	Número de Usuarios que demandan	1000

15. Ficha Técnica para la programación de Adquisiciones Informáticas

15.1. Adquisición de Hardware

Nº	HARDWARE	PRESUPUESTO	CANTIDAD	FINANCIAMIENTO
Servidores				
1	Servidor	25000	1	Propio
Computadoras personales				
2	Computadoras	49500	16	Propio
3	Monitores 19"	38500	16	Propio
Impresoras				
4	Impresora Multifuncional	5500	1	Propio
Otros				
5	Consola KVM LCD 17" 8 Puertos	6000	1	Propio
6	Estabilizadores	4950	15	Propio
7	UPS	5400	9	Propio
8	Ups Sala Servidores	43000	1	Propio
Presupuesto Total Asignado:				S/. 143,200

15.2. Adquisición de Equipos de Comunicación

Nº	HARDWARE	PRESUPUESTO	CANTIDAD	FINANCIAMIENTO
Switches				
1	Switch	33000	3	Propio
Wireless				
2	Acces Point	6000	5	Propio
Presupuesto Total Asignado:				S/. 39,000

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

15.3. Adquisición de Sistemas de Seguridad en Redes y Datos

Nº	HARDWARE	PRESUPUESTO	CANTIDAD	FINANCIAMIENTO
1	Certificado en cableado cat. 6A 4 Garitas	10000	8	Propio
Presupuesto Total Asignado:				S/. 10000

15.4. Adquisición de Software

Nº	SOFTWARE	PRESUPUESTO	CANTIDAD
Herramientas de Desarrollo			
1	Adobe Acrobat Prof	2,280.00	3
2	Soporte Gls Gupta	6,990.00	1
3	Autodesk AEC Collection MultiUser	25,900.00	2
4	ORACLE	5,100.00	2
De Oficina			
10	Microsoft Office Hogar Y	300.00	13
11	Empresas 2016 Microsoft Office Hogar Y Empresas 2019	300.00	9
12	S10 2016	1,600.00	4
13	Correo Institucional	33499.26	140
14	Antivirus Nod 32	8,750.00	250
Diseño			
15	Adobe Cloud Creative Autocad 2020 Lumion 3D Photoshop CC	4,400.00 7,495.00	2 4
Otros			
13	Software de contador de personas	2,548.80	1
14	Sistema de Procesos Judiciales	1,500.00	1

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

15.5. Desarrollo de Sistemas

Nº	SOFTWARE	PRESUPUESTO	FINANCIAMIENTO
Sistema de Información Orientado al ciudadano			
Sistema de Garitas			
Sistema de Tesorería			
Sistema de Presupuesto			
Sistema de Patrimonio			
Sistema de requerimientos (Logística)			
Sistema de Precios (Estadística)			
Sistema de Contabilidad			
1	0	0	Propio
	Tipo de Conexión: Red **Tipo de Desarrollo:** Propios **Tipo de Ámbito:** Internet		
Presupuesto Total Asignado:			S/. 0

SUB-GERENCIA DE INFORMÁTICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

15.6. Adquisiciones de Servicios Informáticos

Nº	SOFTWARE		PRESUPUESTO
1	Mantenimiento Central Telefónica		2000
	Fecha de Inicio 01/06/2019	fecha de Fin	30/06/2020
2	Mantenimiento de Base de Datos		6500
	Fecha de Inicio 01/07/2019	fecha de Fin	31/07/2020
3	Servicio de Internet		22020
	Fecha de Inicio 01/01/2019	fecha de Fin	31/01/2020
5	Mantenimiento de Sala de Servidores		23000
	Fecha de Inicio 01/11/2019	fecha de Fin	31/11/2020
6	Renovación de Licencia Oracle		6500
	Fecha de Inicio 01/06/2019	fecha de Fin	31/06/2020
7	Renovación de Licencia Gupta		5650
	Fecha de Inicio 01/09/2019	fecha de Fin	31/09/2020
8	Renovación de Licencias Antivirus		8750
	Fecha de Inicio 01/04/2019	fecha de Fin	30/04/2020
9	Renovación de Dominio Pagina Web		200
	Fecha de Inicio 30/11/2019	fecha de Fin	30/11/2020
10	Renovación de Licencia de Contador de Personas		2548
	Fecha de Inicio 01/08/2019	fecha de Fin	31/08/2020
11	Renovación de Licencia de SPIJ		1517
	Fecha de Inicio 01/10/2019	fecha de Fin	31/10/2020
12	Servicio de Consulta RENIEC		600
	Fecha de Inicio 01/01/2019	fecha de Fin	31/01/2020
13	Mantenimiento de Sistema de Video Vigilancia		2100
	Fecha de Inicio 01/11/2019	fecha de Fin	31/11/2020
14	Renovación de Correo Google		33000
	Fecha de Inicio 01/09/2019	fecha de Fin	30/09/2020
15	Mantenimiento de Marcador de Asistencia		2000
	Fecha de Inicio 01/10/2019	fecha de Fin	31/10/2020
16	Renovación de Servicio de Custodia		7000
	Fecha de Inicio 01/01/2019	fecha de Fin	31/01/2020
17	Renovación Licencia Fortigate		7400
	Fecha de Inicio 02/05/2019	fecha de Fin	31/05/2020
Presupuesto Total Asignado:			S/. 130,785.00

SUB-GERENCIA DE INFORMÁTICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

15.7. Recursos Humanos a contratar

SUB - ÁREAS

Sugerencia de Informática

Nº	CARGOS	CANTIDAD	PRESUPUESTO
1	Contrato de Personal Apoyo (Desarrollo)	1	42000
2	Contrato de Personal Apoyo (Procesos)	1	45000

15.8. Capacitación y Fortaleza Institucional

Nº	CAPACITACION	PRESUPUESTO	FINANCIAMIENTO
Sistema de Información al personal informático			
1	Capacitación en Java.	30,000	Propio
2	Capacitación en Scrum Fecha de Inicio 05/11/2019 fecha de Fin 30/11/2019 **Tipo de Capacitación:** a Personal Informático		
Presupuesto Total Asignado:			S/. 30,000

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMÍREZ SUB-GERENTE EMMSA

EMPRESA MUNICIPAL DE MERCADOS S.A.
EMMSA

PLAN DE CONTINGENCIA INFORMÁTICO

2019

PLAN DE CONTINGENCIA

Es importante resaltar que para que la organización logre sus objetivos necesita garantizar tiempos de disponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones; de este modo podrá mantener una contingencia eficiente en todas las áreas operativas.

Para la Empresa Municipal de Mercados S.A. es indispensable recurrir a los recursos de cómputo como un medio de proveer información a todos los niveles de la misma, y es de vital importancia que dicha información sea lo más exacta posible.
Por todo lo anteriormente dicho, el estar sin el servicio del computador por un lapso mayor de 3 horas origina distorsiones al funcionamiento normal de nuestros servicios y mayores costos de operación. De continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar las operaciones por falta de información para el control y toma de decisiones de la institución.

En este documento se resalta la necesidad de contar con estrategias que permitan realizar: Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo y recuperación para enfrentar algún desastre. Por lo cual, se debe tomar como Guía para la definición de los procedimientos de seguridad de la Información que cada Gerencia, Sub Gerencia u Oficina de la Empresa debe definir.

Es necesario, por tanto, prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

INDICE

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

1. INTRODUCCION

Conforme ha venido evolucionando la tecnología y con ella la envergadura de los sistemas de información en nuestra Institución, la seguridad del entorno informático (hardware, software, comunicaciones, etc.) se ha convertido en una de las grandes preocupaciones de la Subgerencia de Informática de la Empresa Municipal de Mercados S.A. (EMMSA), siendo esta la encargado de la administración de los recursos informáticos en EMMSA, de su normativa y control. Se ha hecho necesaria la implantación de procedimientos que aseguren y garanticen la operatividad del día a día en caso de desastres o situaciones de riesgo. Esta preocupación debe ser comprendida y compartida por la alta dirección de la empresa, los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad de la empresa.

La necesidad de información de la empresa se ve satisfecha con el manejo de sistemas que garanticen su operatividad y gestión. Esto a su vez se refleja en la optimización de recursos y oportunidad de la información que mantengan competitiva a EMMSA frente a las demás organizaciones.

El Plan de Contingencia desarrollado para EMMSA, implica planificar el reinicio de los procesos críticos de la Subgerencia de Informática, además de determinar las tareas necesarias para reinstalar los sistemas y comunicaciones de las áreas de la empresa.

En la empresa, podrían ocasionarse varios tipos de fallas: mayores, menores, temporales y permanentes. Los procesos podrían dividirse en críticos y complementarios.

En el Plan de Contingencia se contempla el desarrollo de los procedimientos requeridos para resolver tipos de fallas mayores y permanentes que afecten los procesos críticos de EMMSA. Los procedimientos de contingencia contemplan el restablecimiento de la información crítica y las funciones de sistemas y las comunicaciones.

El presente documento es el **Plan de Contingencia** Informático de la Empresa Municipal de Mercados S.A. en materia de Riesgos de Información establece el objetivo, alcance y metodología desarrollada.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

2. Definiciones

Plan de Contingencia: El plan de contingencia es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando aunque sea al mínimo.

3. Objetivos

1. Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
2. Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.
3. Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.
4. Asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.
5. Proteger y conservar los activos de la empresa, de riesgos, desastres naturales o actos mal intencionados.
6. Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
7. Definir las acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

4. Alcances

La Implementación del Plan de Contingencia informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

5. Marco Teórico

El Plan de Contingencia informático es un documento que reúne conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones de EMMSA, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término "incidente" en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático de EMMSA.

Acciones a ser consideradas:

- Antes, como un plan de respaldo o de prevención para mitigar los incidentes.
- Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

a. Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

b. Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

no se encuentra disponible.

Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia. **Se adjunta Formato de ocurrencia de evento.**

c. Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

Todo Plan de Contingencia informático debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

d. Plan de Pruebas

El Plan de Pruebas, será presentado a la Gerencia General de EMMSA para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad.

Las pruebas relacionadas a este plan, se ejecutaría semestralmente, mes de Junio y Diciembre con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar ajustes

6. Organización del Plan de Contingencia

Uno de los aspectos que evidencia un carácter formal y serio en toda organización es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria mientras dure dicho evento.

Es necesario entonces que la definición de un Plan de Contingencia informático deba hacerse de manera formal y responsable de tal forma que involucre en mayor o menor medida a toda la organización en el Plan de Prevención, Ejecución y Recuperación, pero definiendo un *grupo responsable* (Comité de contingencia) para su elaboración, validación y mantenimiento.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Comité de Contingencia

- Gerente de Administración y Finanzas
- Subgerente de Informática
- Subgerente de Logística
- Subgerente de Administración y Mercados
- Subgerente de Seguridad
- Equipo de Trabajo asignado por la Subgerencia de Informática

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

6.1. Funciones Generales del Comité del Plan de Contingencia

- Participar en las reuniones periódicas propuestas por el Coordinador del Plan de Contingencia.
- Proponer la incorporación y/o modificaciones del Plan de contingencia.
- Aprobar y/o rechazar las incorporaciones y/o modificaciones del Plan de Contingencia propuesta por el coordinador de contingencia o sus miembros.
- Verificar que el personal a su cargo se encuentre debidamente capacitado en la ejecución del plan de contingencia.
- Coordinar la ejecución de las actividades del plan de pruebas.
- Aprobar los informes presentados por la coordinación del plan respecto a cualquier evento relacionado con el mismo.
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

6.2. Funciones específicas del Comité del Plan de Contingencia:

Líder del Plan de Contingencia	Gerente de Administración y Finanzas.	Coordinador y responsable de verificar que las actividades de contingencia de sistemas se ejecuten según el plan diseñado y en todos los niveles del proyecto de contingencia.
Administrador del Plan Contingencia:	Sub Gerente de Informática.	Desarrollar el plan de trabajo establecido. Asignar los responsables así como las prioridades para el desarrollo de las tareas. Organizar el proyecto y orientar al equipo de trabajo. Establecer coordinaciones entre el Equipo de trabajo, el Líder del Proyecto y las demás oficinas involucradas. Identificar los problemas, desarrollar las soluciones y recomendar aquellas acciones específicas.
Equipo de Trabajo	• Especialista de Informática • Especialista de Mantenimiento de Equipos • Administrador de Base de Datos. • Sub Gerente de Logística. • Sub Gerente de Seguridad. • Sub Gerente de Administración de Mercados y Sub Administradores.	Ejecutar las acciones encargadas especificadas en el cronograma o plan de trabajo, cumpliendo los plazos señalados a fin de no perjudicar el cumplimiento de las demás tareas. Comunicar oportunamente al Administrador del Proyecto, sobre los avances de las tareas asignadas, así como las dificultades encontradas y la identificación de los riesgos.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

6.3. Contactos del Equipo de Contingencia

NOMBRES Y APELLIDOS	CARGO	EMAIL	TELEFONO
MARIA MELVA GARCIA ATALAYA	Gerente de Administración y Finanzas	mgarciaa@emmsa.com.pe	94496-1477
ISABEL RAMÍREZ SÁNCHEZ	Sub Gerente de Informática	iramirezs@emmsa.com.pe	99647-7793
PATRICIA PEÑA LOAYZA	Especialista de Informática	ppenal@emmsa.com.pe	9873-95917
JEAN PIERRE DIESTRO MANDROS	Administrador de Red	jdiestro@emmsa.com.pe	99330-7156
PAULA ELIZABERTH PEREZ DOMINGUEZ	Sub Gerente de Logística	pperezd@emmsa.com.pe	94340-2369
JOSÉ ONÉSIMO CLAROS SANDY	Sub Gerente de Administración de Mercados	jclaross@emmsa.com.pe	97654-2640
ANGELICA JUAREZ MERA	Gerente de Operaciones	ajuarezm@emmsa.com.pe	94340-2093
ADRIAN ALVARADO BLACIDO	Especialista en Mantenimiento de Equipos	aalvaradob@emmsa.com.pe	94340-2480
DANIEL CANDIOTTI BRAVO	Electricista	dcandiotti@emmsa.com.pe	94653-0895
JORGE MEDINA LOPEZ	Asistente Mantenimiento de Equipos	logistica10@emmsa.com.pe	94433-6351
JHON MUÑOZ COSME	Técnico de Equipos	jmunoz@emmsa.com.pe	95260-9659

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

7. Identificación y Priorización del Riesgo

Para entender los términos a usar en la fase a continuación pasamos a definir algunos conceptos básicos de esta fase.

Incidencia se denomina al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

Riesgo es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas. Es entonces la cuantificación de una amenaza.

Análisis del Riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la probabilidad, impacto y exposición del riesgo. Estos elementos permitirán al equipo coordinador categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

Probabilidad del Riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio. Asimismo, la probabilidad debe ser inferior al 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

La probabilidad se puede entender también como la posibilidad de la consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia será del 100%.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Impacto del Riesgo

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia.

Es una calificación aplicada al riesgo, para describir su impacto en relación

al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto.
Para nuestro caso, clasificaremos el impacto con una escala del 1 al 4.

Eventos Controlables, si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado.

Eventos No Controlables, cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio.
Esta identificación se hará en la matriz de riesgo explicada a continuación.

7.1. Definición de la Matriz de Riesgo

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas de las actividades de las Gerencias y Sub Gerencias de EMMSA en tal sentido, resulta vital conocer el impacto del evento cuando este se presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser muy objetivos en su análisis.

Cuadro 1: Detalle del Valor del Impacto

Impacto	Descripción	Valor
Poco Impacto	Pérdida de Información y/o equipamiento no sensible	**1**
Moderado Impacto	Pérdida de información sensible	**2**
Alto Impacto	Pérdida de información sensible, retraso o interrupción	**3**
Gran Impacto	Información crítica, daño serio, patrimonial	**4**

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Cuadro 2: Detalle de la Probabilidad de la Ocurrencia

Impacto	Descripción
Frecuente	Incidentes repetidos
Probable	Incidentes aislados
Ocasional	Sucede alguna vez
Remoto	Improbable que suceda

SUB-GERENCIA DE INFORMATICA V°B° L. RAMIREZ SUB-GERENTE EMMSA

7.2. Identificación de Riesgos (Matriz)

Tipo Riesgo Codificado	#	Descripción	Probabilidad de Ocurrencia	Impacto
INFRAESTRUCTURA CODIGO SI-PC-1	1	Incendio	Remoto	4
	2	Sismo	Probable	4
	3	Inundación tuberías del GMML - Centro Comercial.	Remoto	3
	4	Sabotaje Informático	Remoto	3
	5	Robo	Probable	3
SERVICIO PUBLICOS CODIGO SI-PC-2	1	Cortes de Energía Publica	Ocasional	3
	2	Corte de línea de Telefonía	Ocasional	3
	3	Corte de Energía electica por mantenimiento en las Subestaciones 2 y 3	Ocasional	3
EQUIPOS TELECOMUNICACIONES y TELEFONIA CODIGO SI-PC-3	1	Falla de Equipo Firewall	Remoto	2
	2	Falla de Switch de la Sala de Telecomunicaciones	Remoto	2
	3	Falla de Equipo Router de Internet	Remoto	2
	4	Falla de la Central Telefónica	Remoto	2
	5	Falla de Switch de Red de 1er, 2do. y 3er Piso.	Probable	3
SERVIDORES CODIGO SI-PC-4	1	Falla del Hw o Sistema Operativo de los Servidores	Probable	4
BASE DE DATOS CODIGO SI-PC-5	1	Falla en las Base de Datos Oracle, SQL de los servidores.	Probable	4
SOFTWARE CODIGO SI-PC-6	1	Falla de aplicativos propios de EMMSA.	Probable	3
	2	Infección de Equipos por Falla o Vencimiento de Licencias ANTIVIRUS	Probable	3
CORREO ELECTRONICO CODIGO SI-PC-7	1	Suspensión de Servicio de Correo Electrónico GMAIL	Probable	3
INFORMACION CODIGO SI-PC-8	1	Sustracción o Robo de Información	Probable	3

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

RECURSO HUMANO CODIGO SI-PC-9	1	Ausencia imprevista del Personal Informático	Probable	3
	2	Falta de idoneidad del personal respecto a la Información de la Base de Datos.	Remoto	3
SISTEMA DE VIDEO VIGILANCIA CODIGO SI-PC-10	2	Fallas de Grabación de los NVRs.	Probable	3
	1	Fallas de Cámaras Domos o Fijas	Probable	3
	3	Fallas de Equipos de Monitoreo	Probable	3
RECURSOS DE COMPUTO Y OPERATIVOS CODIGO SI-PC-11	1	Falla de Computadoras, Impresoras, Escáner, Marcadores de Huella.	Ocasional	3
	2	Falla de Aire Acondicionado del TELECOM.	Ocasional	2
	3	Falla de UPS Telecom y otros	Ocasional	2
	4	Falla de Grupo Electrógeno	Probable	3

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

7.3. Eventos Controlables

EQUIPOS TELECOMUNICACIONES y TELEFONIA	1	Falla de Equipo Firewall
	2	Falla de Switch de Comunicaciones
	3	Falla de Equipo Router de Internet
	4	Falla de la Central Telefónica
	5	Falla de Switch de Red de 1er, 2do. Y 3er Piso.
SERVIDORES	1	Falla del Hw o Sistema Operativo de los Servidores
BASE DE DATOS	1	Falla en las Base de Datos Oracle, SQL de los servidores.
SOFTWARE	1	Falla de aplicativos propios de EMMSA.
	2	Infección de Equipos por Falla o Vencimiento de Licencias ANTIVIRUS
CORREO ELECTRONICO	1	Suspensión de Servicio de Correo Electrónico GMAIL
INFORMACION	2	Sustracción o Robo de Información
RECURSO HUMANO	1	Ausencia imprevista del Personal Informático
SISTEMA DE VIDEO VIGILANCIA	1	Fallas de Grabación de los NVRs.
	2	Fallas de Cámaras Domos o Fijas
	3	Fallas de Equipos de Monitoreo
RECURSOS DE COMPUTO Y OPERATIVOS	1	Falla de Computadoras, Impresoras, Escaners, Marcadores de Huella.
	2	Falla de Aire Acondicionado del TELECOM.
	3	Falla de UPS Telecom y otros
	4	Falla de Grupo Electrógeno

7.4. Eventos No Controlables

SERVICIO PUBLICOS	1	Cortes de Energía Publica
	2	Corte de línea de Telefonía
INFRAESTRUCTURA	1	Incendio
	2	Sismo
	3	Inundación tuberías del GMML – Centro Comercial.
	4	Sabotaje
INFORMACION	2	Sustracción o Robo de Información
	2	Falta de idoneidad del personal respecto a la Información de la Base de Datos.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

7.5. Impacto

IMPACTO	ÁREA AFECTADA
1. Caída de la Red LAN: Servidores Windows, equipos de comunicación.	Todas las Áreas
2. Interrupción de las comunicaciones Internas y Externas.	Todas las Áreas
3. Paralización de los sistemas que soportan las funciones de la Institución.	Todas las Áreas
4. Paralización de operaciones de Informática.	Todas las Áreas
5. Perdida de Hardware y Software.	Tecnología de la Información

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

8. **Recursos Informáticos susceptibles a contingencia:**
Actualmente la Subgerencia de Informática cuenta con los siguientes con recursos informáticos:

8.1. Servidores Físicos por Tipo

DESCRIPCION DE SERVIDORES		Nº	1	2	3
		FUNCION	**Servidor de Archivos**	**Servidor de Base de Datos**	**Servidor de Trámite Documentario**
		TIPO	SERVIDOR	SERVIDOR	SERVIDOR
		HOSTNAME	ORAEMMSA	EMMSADB	GESDOC
		IP ADDRESS	10.60.0.4	10.60.0.2	10.60.0.6
		APLICACIONES	Archivos, Documentos, etc.	Base de Datos Oracle SAFIM	Apache, MySql
	CARACTERISTICAS	SISTEMA OPERATIVO	Windows Server 2003 Standar Edition	Windows Server 2012StandarEdition	Linux Centos 6.3
		MODELO	HP PROLIANT ML 150G5	HP	Dell PowerEdge R620
		PROCESADOR	Intel Xeon 5405	Intel XeonES-2403	Intel XeonE5-2609 2.4Ghz
		ESTADO	Operativo	Operativo	Operativo

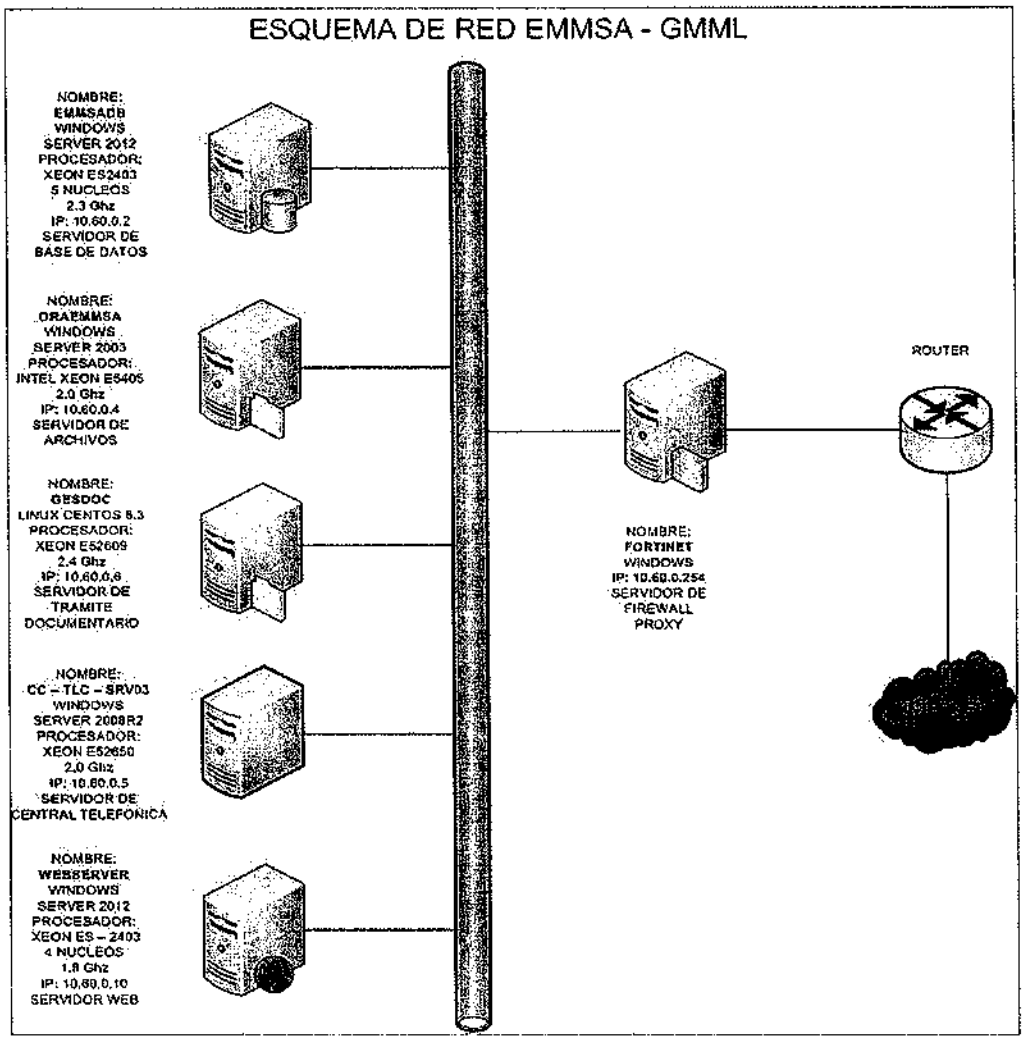
SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

DESCRIPCION DE SERVIDORES	Nº	4	5	6
CARACTERISTICAS	FUNCION	**Servidor Marcador de Personal**	**Servidor Web**	**Servidor Back Up**
	TIPO	SERVIDOR	SERVIDOR	SERVIDOR
	HOSTNAME	CC-TLC-SRV03	WEBSERVER	SERVIDOR
	IP ADDRESS	10.60.0.5	10.70.104	10.60.0.9
	APLICACIONES	Base de Datos Oracle TECFLEX	PAGINA WEB	BACK UP
	SISTEMA OPERATIVO	Windows Server 2008R2 Standard	Windows Server 2012	Linux Centos 6.3
	MODELO	Dell PowerEdge R620	HP Proliant DL 360e Gen8	Dell PowerEdge R710
	PROCESADOR	Intel XeonE5-2650 2Ghz	Intel XeonES-2403	Intel Xeon 5500
	ESTADO	Operativo	Operativo	Operativo

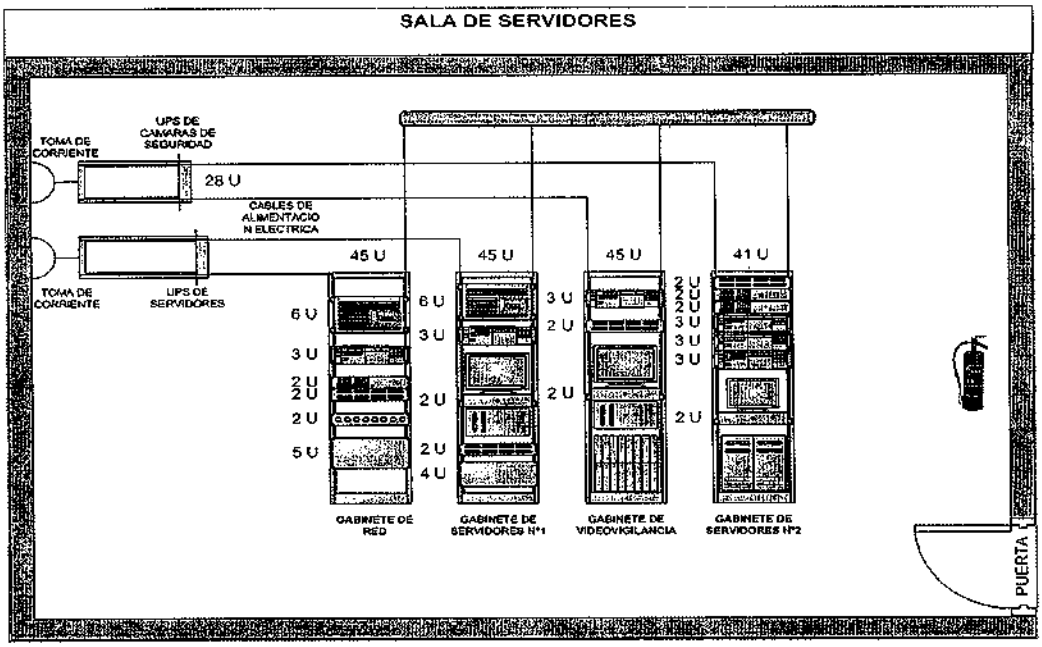
SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

8.2. Sala de TELECOM

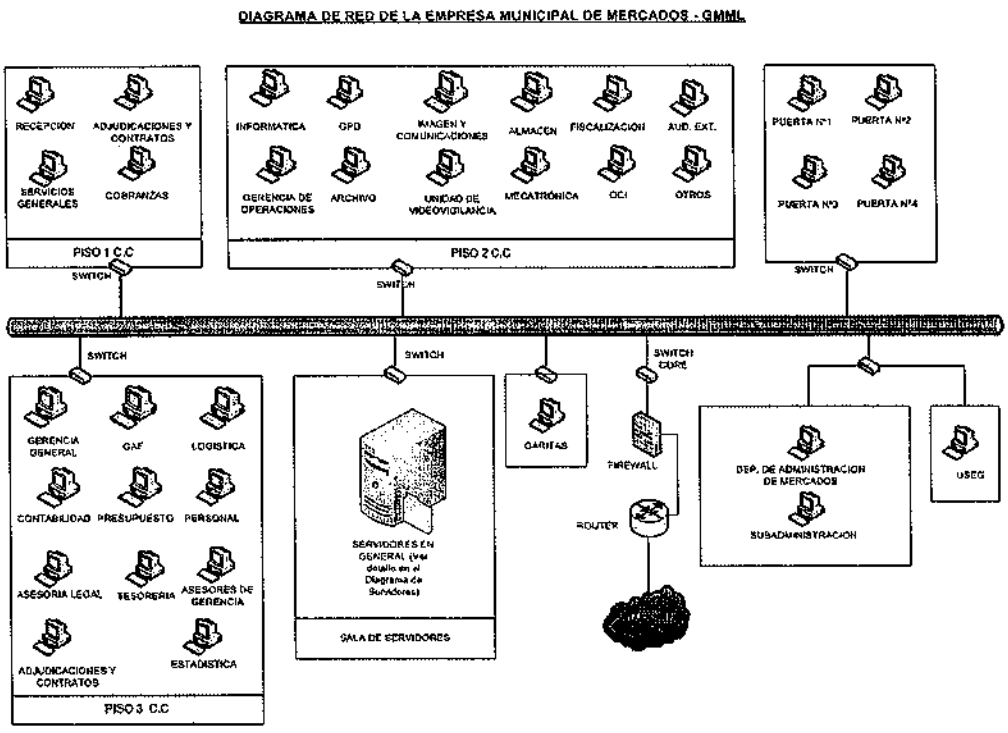
Los Servidores se encuentran en la sala de Telecomunicaciones 1er Piso del Centro Comercial.



SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB GERENTE
EMMSA



8.3. Equipos de cómputo y Diagrama de Red



8.4. El Sistema de Video Vigilancia CCTV-GMML

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

El Sistema integral de video vigilancia está conformado por una plataforma basada en conectividad IP, el cual integra cámaras DOMO PTZ, cámaras fijas, backbone de fibra óptica para interconexión de las cámaras con el centro de control, cableado estructurado para datos, estación de monitoreo y control, matriz virtual para visualización y despliegue de las cámaras, sistemas de grabación NVR con arreglos de discos para su almacenamiento, plataforma de gestión (manejo de usuarios, perfiles, dispositivos, etc.), sistema de protección antes cortes de energía eléctrica (UPS).A continuación se detalla los componentes del sistema instalado:

- Plataforma de grabación NVR
- Estación de monitoreo y Control
- Cámaras IP
- Matriz Virtual

HDNVR1	10.30.0.140/24	10.30.0.1	Administrator
NVR Domos	10.30.0.29/24	10.30.0.1	Administrator
HDNVR2	10.30.0.141/24	10.30.0.1	Administrator
Operador 1	10.30.0.26/24	10.30.0.1	Estacion1
Operador 2	10.30.0.142/24	10.30.0.1	Estacion2
Operador 3	10.30.0.143/24	10.30.0.1	Estacion3
VideoWall Avigilon	10.30.0.115/24	10.30.0.1	VideoWall

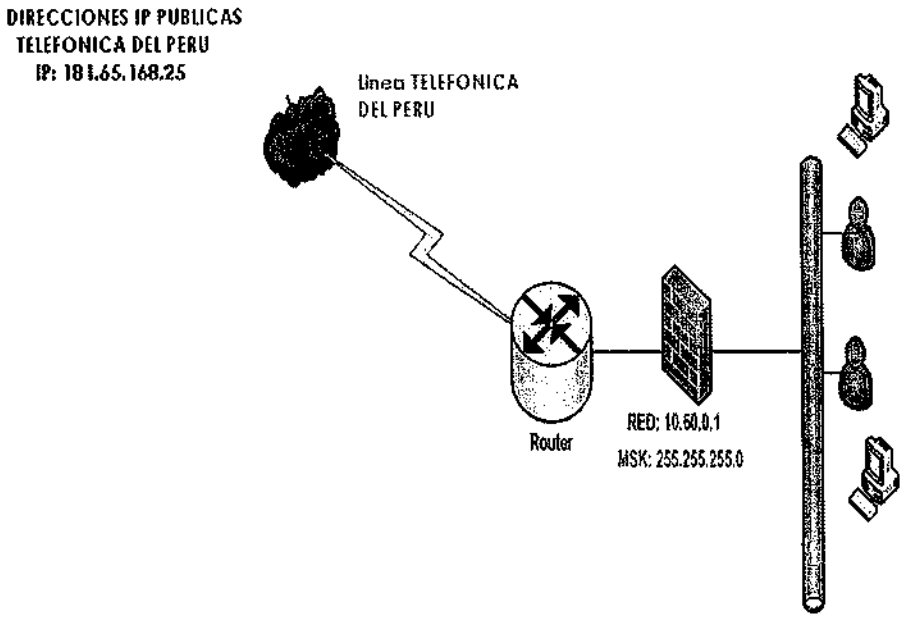
Se adjunta relación de cámaras

8.5. Servicio de Internet EMMSA.

Actualmente se tiene el contrato de servicio de internet por un plazo de 2 años y con ancho 10 MEGAS.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

8.6. Correo electrónico EMMSA



Actualmente este servicio esta tercerizado con Google Apps asociado a nuestro dominio empresarial con un total de 125 cuentas habilitadas de correo.

Características

Almacenamiento de Gmail + Google Drive	30 GB/cuenta
Interoperabilidad con el correo electrónico y el calendario de Microsoft Outlook	✔
Sincronización con BlackBerry Enterprise Server	✔
Administración sencilla de contactos	✔
Acceso a las aplicaciones de mensajería instantánea, de calendario y de correo electrónico para móviles	✔
Posibilidad de inhabilitar los anuncios	✔

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

de Gmail	
Programación de recursos en Google Calendar	✔
Funciones de lista de distribución y herramientas que permiten compartir contenido con grupos fácilmente	✔

Aplicaciones de colaboración: Google Docs, Google Sites y Google Video for Business
Mayor seguridad

Aplicación de SSL para un acceso HTTPS seguro	✔
Filtrado de spam personalizable	✔
Personalización de los requisitos de seguridad de la contraseña	✔
Asistencia para la pasarela y la redirección del correo electrónico	✔

Se adjunta relación de correos electrónicos

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

9. Elaboración de los Planes de Contingencia

Una de las fases importantes del Plan de Contingencia es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento es por ello que se considerara un formato de registro de los eventos definidos que forman parte del plan. El contenido de todos los eventos que conformarán el Plan de Contingencia son:

"Formulario de registro del Plan de Contingencia", el mismo que describimos a continuación y que se compone de las siguientes partes:

Elaborado: Sub Gerencia de Informática EMMSA S.A.
Código del Formato: SI-PC-Tipo de Riesgo Codificado-# (Según Matriz)
Nombre del Evento: Claro y de fácil entendimiento.
Cuerpo Principal: Contenido del evento y que forman parte del Plan de Contingencia.

(Ver Página del 29 al 33).

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

9.1. Definición y alcance del Plan de Pruebas

Conscientes que una situación de contingencia extrema puede presentarse en cualquier momento, y por ende convertirse en un problema prioritario de atender dado que el Gran Mercado Mayorista funciona los 365 días del año y las 24 horas del día por lo que se hace necesario definir de manera específica todas las acciones necesarias para asegurar que, en caso real de contingencia y tener un conjunto de prestaciones y funcionalidades mínimas que permitan posteriormente ejecutar el plan de recuperación de manera rápida y segura. Por ello se deberá realizar las siguientes actividades.

- Programar la prueba y validación de todas las actividades que se llevarán a cabo como parte del Plan de Ejecución del Plan de Contingencia respecto a una posible interrupción de los procesos identificados como críticos de EMMSA.
- Identificar por medio de la prueba, las posibles causas que puedan atentar contra su normal ejecución y las medidas correctivas a aplicar para subsanar los errores o deficiencias que se deriven de ella (retroalimentación del plan).
- Determinar los roles y funciones que cumplirán el equipo de trabajo en la prueba, los mismos que serán los asignados para su ejecución en caso de una situación real de contingencia.
- Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por un grupo determinado de usuarios que podrán ser los de roles críticos de algunos procesos de las Gerencias y Subgerencias de EMMSA, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.
- Se diseñara un **formato de las pruebas** del Plan de Contingencia que se adjunta a continuación.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Objetivo de la Prueba del Plan de Contingencia	Definición de Objetivos
Alcance	Gerencias y Subgerencias afectadas y personal involucrado de EMMSA.
Descripción de la pruebas a efectuarse	Evento a realizar las pruebas.
Resultados Esperados de las pruebas.	Relación de acciones
Fecha y Hora	De la prueba realizada
Responsable de las Pruebas del Plan	Subgerencia de Informática
Tipo Riesgo Codificado	Descripción de las pruebas del Tipo de Riesgo Codificado

(Ver anexo)

9.2. Validación y Registro de Pruebas

Todas las actividades generales que forman parte de la prueba, deberán validarse, registrarse (incluyendo observaciones) y firmarse por todos los responsables que participaron en cada una de ellas, a fin de dar fe de su ejecución y certificación.

Se diseñara un formato de Control y Certificación de Pruebas de Contingencia que se usará para la validación y registro de las pruebas.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

10. Plan de Pruebas de la Matriz de Riesgo

Evento : **Incendio**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Seguridad de EMMSA y se registrara en el formato de pruebas del plan de contingencias.		
Evento : **Sismo**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.2** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Seguridad de EMMSA y se registrara en el formato de pruebas del plan de contingencias.		
Evento : **Inundación tuberías del GMML – Centro Comercial.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.3** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Logística de EMMSA y se registrara en el formato de pruebas del plan de contingencias		
Evento : **Sabotaje Informático**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.4** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Seguridad de EMMSA y se registrara en el formato de pruebas del plan de contingencias.		
Evento : **Robo**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.5** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Seguridad de EMMSA y se registrara en el formato de pruebas del plan de contingencias.		

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Corte de Energía Publica**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-2.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Logística y se registrara en el formato de pruebas del plan de contingencias.		
Evento: **Corte de línea de Telefonía**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-2.2** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Logística y se registrara en el formato de pruebas del plan de contingencias.		
Evento: **Falla de Equipo Firewall**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falla de Switch de la Sala de Telecomunicaciones**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.2** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falla de Equipo Router de Internet**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.3** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falla de la Central Telefónica**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.4** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con la Subgerencia de Logística y se registrara en el formato de pruebas del plan de contingencias.		
Evento:	Entidad Responsable	**SI-PC-3.5**

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Falla de Switch de Red de 1er, 2do. y 3er Piso.	Involucrada: **EMMSA**	FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falla del Hw o Sistema Operativo de los Servidores**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-4.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falla en las Base de Datos Oracle, SQL de los servidores.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-5.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falla de aplicativos propios de EMMSA.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-6.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Infección de Equipos por Falla o Vencimiento de Licencias ANTIVIRUS**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-6.2** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Logística.		
Evento: **Suspensión de Servicio de Correo Electrónico GMAIL**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-7.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Logística.		
Evento: **Sustracción o Robo de**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-8.1**

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Información		FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Seguridad.		
Evento: **Ausencia imprevista del Personal Informático**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-9.1** FECHA: Versión:
El plan de pruebas se realizara por el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falta de idoneidad del personal respecto a la Información de la Base de Datos.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-9.2** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática.		
Evento: **Falla de Cámaras Domos o Fijas**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-10.1** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Seguridad.		
Evento: **Falla de Grabación de los NVRs**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-10.2** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Seguridad.		
Evento: **Falla de Equipos de Monitoreo**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-10.3** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Seguridad.		

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento: **Computadoras, impresoras**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.1** FECHA: Versión:

equipos, marcador huellas		
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Seguridad.		
Evento: **Falla de Computadoras, Impresoras, Escáner, Marcadores de Huella.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.2** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Logística.		
Evento: **Falla de Aire Acondicionado de TELECOM**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.3** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Logística.		
Evento: **Falla de UPS de TELECOM**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.4** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Logística.		
Evento: **Falla de Grupo Electrógeno**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.4** FECHA: Versión:
El plan de pruebas se realizara el comité de contingencia en coordinación con el equipo de la Subgerencia de Informática y la Subgerencia de Logística.		

11. Plan de Prevención y Plan de Recuperación de la Matriz de Riesgo

Evento : **Incendio**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.1** FECHA: Versión:

1. Plan de Prevención

Descripción del Evento:

Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura

- Sala de Telecomunicaciones
- Oficinas de Gerencias y Subgerencias de EMMSA.

Recursos Humanos

- Personal debidamente entrenado para afrontar el evento

Objetivo

Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones de EMMSA sin exponer la seguridad de las personas.

Criticidad

EMMSA determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

Entorno

Este evento se puede dar en las instalaciones de las Gerencias y Subgerencias de EMMSA y en los pabellones del Gran Mercado Mayorista de Lima.

Personal Encargado

El Subgerente de Informática es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Condiciones de Prevención de Riesgo

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Charlas sobre el uso y manejo de extintores de cada uno de los tipos.
- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal de EMMSA responsable de las acciones de prevención y ejecución de la contingencia.

Igualmente se deberá contar con los siguientes elementos para la detección y extinción de un posible incendio, los cuales cubrirán los ambientes de la SALA DE TELECOMUNICACIONES de EMMSA, por lo que se deberá

Implementar detectores de humo
Mantener actualizado los extintores

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

La Contingencia se activará al ocurrir un incendio.

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

Procesos Relacionados antes del evento.

- Identificar la alarma contra incendio.
- Identificar la ubicación de los extintores.
- Conocer el número de emergencia de la Subgerencia de Seguridad de EMMSA.
- Tener número de teléfono del personal responsable del personal de la Subgerencia de Informática y del equipo de Contingencia de EMMSA.
- Conocer el número de emergencia de los bomberos.

Personal que autoriza la contingencia.

El Gerente de Administración y Finanzas o el Subgerente de Informática pueden activar la contingencia.

Descripción de las actividades después de activar la contingencia.

- Tratar de apagar el incendio con extintores.
- Comunicar al personal responsable de EMMSA.
- Evacuar el área.
- En todo momento se coordinará con el Comité de Contingencia y La Subgerencia de Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de extinguido el incendio, se deberán realizar las siguientes actividades:

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

- Evaluación de los daños ocasionados al personal, bienes e instalaciones.
- En caso de daños del personal prestar asistencia médica inmediata
- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- En caso se haya detectado bienes afectados por el evento, se evaluará el Caso para determinar la reposición o restauración.

La Coordinación Ejecutora del Plan de Co ntingencias deberá coordinar con la Alta Dirección de EMMSA en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectado.

Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio.

Evento : **Sismo**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.2** FECHA: Versión:

1. PLAN DE PREVENCIÓN

Descripción del evento

Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Infraestructura

- Oficinas de EMMSA
- Personal

Objetivo

Establecer las acciones que se tomarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del IMARPE evitando exponer la seguridad de las personas.

Criticidad

EMMSA determina este evento tiene un nivel de gran impacto en el servicio y se identifica

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

como CRITICO.

Entorno

Este evento se puede dar en las instalaciones de EMMSA.

Personal Encargado

El Gerente General o Gerente o Subgerente de cada área, en este caso nos alineáramos a lo indicado por el Personal de la Subgerencia de Seguridad de EMMSA.

Condiciones de Prevención de Riesgo

- Contar con un plan de evacuación de las instalaciones de EMMSA, el mismo que debe ser de conocimiento de todo el personal que labora.
- Participara de los simulacros de evacuación con la participación de todo el Personal.
- Mantener las salidas libres de obstáculos.
- Señalizar todas las salidas.
- Señalizar las zonas seguras.
- Definir los puntos de reunión en caso de evacuación.

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia • Sismo.

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

Procesos Relacionados antes del evento.

- Tener la lista de los empleados por Gerencias y Subgerencias actualizadas
- Mantenimiento del orden y limpieza.
- Inspecciones diarias de seguridad interna.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades

Personal que autoriza la contingencia.

El Gerente General y el Gerente de Administración y Finanzas pueden activar la contingencia

Descripción de las actividades después de activar la contingencia.

- Desconectar el fluido eléctrico.
- Evacuar las oficinas de acuerdo a las disposiciones del Gerente General y el Gerente de Administración y Finanzas utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

- Verificar que todo el personal de EMMSA que labora en el área se encuentren bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario. (
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo y equipos de cómputo.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo.
- En todo momento se coordinará con las otras Gerencias y Subgerencias de EMMSA De las acciones que deban ser efectuadas por ellos.

.

Duración

La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El personal encargado del Plan de Recuperación es la Gerencia y Subgerencias afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la Institución.

Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible la el trabajo informático durante la interrupción del servicio.

Mecanismos de Comprobación

El Subgerente de Informática evaluara las pérdidas de equipos del evento.

Desactivación del Plan de Contingencia

El Gerente General y/o el Gerente de Administración y Finanzas desactivarán el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica.

Proceso de Actualización

El proceso de actualización será en coordinación con la Subgerencia de Seguridad y el Subgerente de Informática quien determinará las acciones a tomar.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Inundación tuberías del GMML – Centro Comercial.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.3** FECHA: Versión:

3. Plan de Prevención

Descripción del Evento:

Es un evento de inundación de agua producto de una rotura o desborde de tuberías de las conductos de agua del 1er, 2do o 3er Piso de las Oficinas Administrativas y que perjudica los equipos de comunicación ubicados en la Sala de Telecomunicaciones (TELECOM).

Este evento incluye los siguientes elementos mínimos identificados por EMMSA, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura

- Sala de Telecomunicaciones

Recursos Humanos

- Personal debidamente entrenado para afrontar el evento

Objetivo

Establecer las acciones que se ejecutaran ante inundaciones de tuberías a fin de minimizar el tiempo de interrupción de las operaciones de EMMSA sin exponer la vida útil de los equipos de comunicaciones.

Criticidad

EMMSA determina que el presente evento tiene un nivel de Alto Impacto.

Entorno

Este evento se puede dar en la Sala de Telecomunicaciones o en otras instalaciones de EMMSA.

Personal Encargado

El Subgerente de Informática y el Subgerente de Logística es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

Condiciones de Prevención de Riesgo

- Prevenir acciones o trabajos que puedan ocasionar rupturas de las tuberías cerca de la Sala de Telecomunicaciones.
- Consultar con la Subgerencia de Informática sobre modificaciones a realizar de trabajos de mantenimientos de infraestructura de las Oficinas Administrativas.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

4. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

La Contingencia se activará al ocurrir una inundación en las Oficinas Administrativas.

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

Procesos Relacionados antes del evento.

- Identificar las llaves generales de agua de las Oficinas Administrativas.
- Tener número de teléfono del personal responsable del personal de la Subgerencia de Informática y del equipo de Contingencia de EMMSA.

Personal que autoriza la contingencia.

El Gerente de Administración y Finanzas o el Subgerente de Informática pueden activar la contingencia.

Descripción de las actividades después de activar la contingencia.

- Mantener cerradas las llaves de agua hasta verificar que no hay goteo o filtro de agua en la Sala de Telecomunicaciones.
- Limpiar y Evacuar los equipos de la Sala de Telecomunicaciones.
- En todo momento se coordinará con el Comité de Contingencia y La Subgerencia de Logística las acciones que deban ser efectuadas por ellos.

Luego de subsanar las roturas de tuberías se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados de bienes e instalaciones.
- Verificar el funcionamiento de los equipos ubicados en la Sala de Telecomunicaciones.
- En caso se haya detectado equipos de comunicaciones afectados por el evento, se evaluará el Caso para determinar la reposición o restauración.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección de EMMSA en caso se requiera la habilitación de ambientes provisionales alternos para restablecer la función de los ambientes afectado.

Duración

La duración de la contingencia dependerá del tiempo que demande controlar la inundación de agua.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento	Entidad Responsable Involucrada	SI-PG-1.4
Sabotaje Informático	EMMSA	FECHA Versión

1. Plan de Prevención

Descripción del Evento:

La acción de sabotaje informático comprende todas aquellas conductas dirigidas a eliminar o modificar funciones o datos en una computadora sin autorización, para obstaculizar su correcto funcionamiento, es decir, causar daños en el hardware o en el software de un sistema.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura

- Servidores
- Computadoras de los usuarios.
- Infraestructura de Red.

Recursos Humanos

• Personal de Subgerencia de Informática y la Subgerencia de Seguridad debidamente entrenado para afrontar el evento.

Objetivo

Establecer las acciones que se ejecutaran ante un sabotaje informático a fin de minimizar las consecuencias y el tiempo de interrupción de las operaciones de EMMSA.

Criticidad

EMMSA determina que el presente evento tiene un nivel de Alto impacto en el Servicio.

Entorno

Este evento se puede dar en las oficinas de las Gerencias y Subgerencias de EMMSA.

Personal Encargado

El Subgerente de Informática es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

Condiciones de Prevención de Riesgo

- Aplicar las políticas de seguridad informática establecidas en las directivas por la

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Subgerencia de Informática.

- Establecer seguridad física en la sala de servidores y en todos los gabinetes de equipos de red.
- Establecer las políticas de seguridad en la creación de usuarios y sus accesos a los diferentes recursos informáticos.

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

La Contingencia se activará al ocurrir la detección del sabotaje informático.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.
Procesos Relacionados antes del evento.

- Identificar el equipo donde ocurrió el sabotaje informático.
- Identificar la sustracción de información o corrupción de archivos.
- Informar a la Subgerencia de Seguridad por si el sabotaje fuera de una persona ajena.
- Informar a la Subgerencia de Recursos Humanos por si el sabotaje fuera del personal que labora en EMMSA.
- Solicitar los videos de seguridad de las instalaciones cerca al evento ocurrido a la Subgerencia de Seguridad.
- Tener número de teléfono del personal responsable del personal de la Subgerencia de Informática y del equipo de Contingencia de EMMSA.

Personal que autoriza la contingencia.

El Gerente de Administración y Finanzas o el Subgerente de Informática pueden activar la contingencia.

Descripción de las actividades después de activar la contingencia.

- Cambiar Claves de Seguridad.
- Verificar los accesos físicos a los equipos vulnerados.
- Comunicar al personal responsable de EMMSA.
- En todo momento se coordinará con el Comité de Contingencia y La Subgerencia de Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de haber superado el sabotaje informático , se deberán realizar las siguientes actividades:

- Evaluación de los daños ocasionados.
- En caso se haya detectado los bienes afectados por el evento, se evaluará el

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Caso para realizar los cambios de seguridad respectivas.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección de EMMSA en caso se requiera las sanciones y medidas aplicadas según reglamento.

e. Duración

La duración de la contingencia dependerá del tiempo que demande controlar o perjudique el sabotaje informático.

Evento : **Robo**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-1.5** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del Evento:

El **robo** es un delito contra el patrimonio, consistente en la sustracción en este caso de software o hardware de la .Este evento incluye los siguientes elementos mínimos identificados por EMMSA, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Hardware y Software

- Licencias
- Computadoras, Impresoras, Laptops, Usb, Cds.
- Herramientas de soporte técnico.

Recursos Humanos

• Personal de Subgerencia de Informática y la Subgerencia de Seguridad debidamente entrenado para afrontar el evento.

Objetivo

Establecer las acciones que se ejecutaran ante un robo a fin de minimizar las consecuencias y el tiempo de interrupción de las operaciones de EMMSA.

Criticidad

EMMSA determina que el presente evento tiene un nivel de Alto impacto en el Servicio.

Entorno

Este evento se puede dar en las oficinas de las Gerencias y Subgerencias de EMMSA.

Personal Encargado

El Subgerente de Informática y todo el personal de la empresa es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Condiciones de Prevención de Riesgo

- Aplicar las políticas de seguridad informática establecidas en las directivas por la Subgerencia de Informática.
- Establecer seguridad física en todos los ambientes del área de informática y/o otras áreas donde se encuentren equipos informáticos.

3. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

La Contingencia se activará al ocurrir la detección del robo de Hw y Sw.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.
Procesos Relacionados antes del evento.

- Identificar los equipos y las áreas de donde han sido sustraídos los.
- Identificar los usuarios que utilizaban estos equipos.
- Informe de los usuarios a la Subgerencia de Seguridad.
- Solicitar los videos de seguridad de las instalaciones cerca al evento ocurrido a la Subgerencia de Seguridad.
- Tener número de teléfono del personal responsable del personal de la Subgerencia de Informática y del equipo de Contingencia de EMMSA.

Personal que autoriza la contingencia.

El Gerente de Administración y Finanzas o el Subgerente de Informática pueden activar la contingencia.

Descripción de las actividades después de activar la contingencia.

- Verificar los accesos físicos a los equipos vulnerados.
- Verificar las pólizas de seguro si las hubiera en coordinación con la Subgerencia de Logística.
- Comunicar al personal responsable de EMMSA.
- En todo momento se coordinará con el Comité de Contingencia y La Subgerencia de Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de haber superado el robo , se deberán realizar las siguientes actividades:

- Actualizar el inventario de equipos.
- En caso de no poder reemplazar los equipos de mayor demanda que han sido sustraídos realizar un plan de reposición en coordinación con la GAF Y Subgerencia de Logística.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección de EMMSA en caso se requiera las denuncias respectivas en coordinación con la Subgerencia de Seguridad.

f. Duración

La duración de la contingencia dependerá del tiempo que demande reemplazar los equipos más necesarios y que han sido sustraídos.

Evento : **Corte de Energía Publica**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-2.1** FECHA: Versión:

1. PLAN DE PREVENCIÓN

Descripción del evento

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos

Suministro de Energía Eléctrica **Hardware**

- Servidores
    - Estaciones de Trabajo ,Equipos Diversos ,PS

Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante la operatividad, afectando el fluido eléctrico de las instalaciones de EMMSA.

Personal Encargado

El Gerente de Administración y Finanzas y el Subgerente de Informática son responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 30 minutos como máximo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realizar con la Subgerencia de Logística pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Contar con UPS para proteger los servidores de correo y desarrollo, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.
- Contar con UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación)

• Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones informáticas.

2. PLAN DE EJECUCIÓN

a. Eventos que activan la Contingencia
Corte de suministro de energía eléctrica en los ambientes de EMMSA.

b. Procesos Relacionados Antes del evento.
Cualquier actividad de servicio dentro de las instalaciones de EMMSA.

c. Personal que autoriza la contingencia
El Gerente de Administración y Finanzas y el Subgerente de Informática pueden activar la contingencia.

d. Descripción de las procedimientos después de activar la contingencia

- Informar al Gerente de Administración y Finanzas el problema presentado.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de apli+caciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS's, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.
- En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción, desarrollo hasta que regrese el fluido eléctrico.

Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

energía eléctrica.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Subgerente de Informática se encargará de realizar las acciones de recuperación necesarias.

Descripción

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Se informará al Comité de Contingencia el Plan el problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso.

Mecanismos de Comprobación

El Gerente de Administración y Finanzas y/o Subgerente de Informática presentará un informe explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Desactivación del Plan de Contingencia

El Gerente de Administración y Finanzas y/o Subgerente de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar.

Evento : **Corte de línea de Telefónica**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-2.2** FECHA: Versión:

1.PLAN DE PREVENCIÓN

Descripción del evento

Este evento refiere al servicio ofrecido por el proveedor de telefonía para la comunicación de los usuarios de EMMSA.

Hardware

Central Telefónica y Equipos de Anexos

Software

Software de Central Telefónica

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Objetivo

Restaurar las funciones de acceso telefónico para la comunicación de la empresa.

Criticidad

Este evento se considera de Alto Impacto.

Entorno

Se puede producir durante la operatividad, afectando las comunicaciones de EMMSA.

Personal Encargado

El Subgerente de Informática y el Subgerente de Logística son responsables de realizar las coordinaciones para restablecer de Corte de Línea Telefónica.

Condiciones de Prevención de Riesgo

- Coordinar con la Subgerencia de Logística sobre la puntualidad de pagos del servicio.
- Contar con equipos adicionales que puedan ser utilizados en caso de falta de línea en la central telefónica.

3. PLAN DE EJECUCIÓN

b. Eventos que activan la Contingencia

Falta de línea telefónica en la central telefónica de EMMSA.

c. Procesos Relacionados Antes del evento.

Cualquier actividad de servicio dentro de las instalaciones de EMMSA.

d. Personal que autoriza la contingencia

El Gerente de Administración y Finanzas y el Subgerente de Informática pueden activar la contingencia.

e. Descripción de las procedimientos después de activar la contingencia

- Informar al Gerente de Administración y Finanzas el problema presentado.
- Dar aviso del corte de línea telefónica en forma oportuna a todas las áreas y coordinar las acciones necesarias.
- Tener un numero alterno que deba ser anexado a la central telefónica y poder continuar con la operatividad por lo menos en recepción y/o mesa de partes.

Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor externo que habilite la línea telefónica.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Subgerente de Informática en coordinación con el Subgerente de Logística se encargará de realizar las acciones de recuperación necesarias.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Descripción

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Se informará al Comité de Contingencia el Plan el problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso.

Mecanismos de Comprobación

El Gerente de Administración y Finanzas y/o Subgerente de Informática presentará un informe explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Desactivación del Plan de Contingencia

El Gerente de Administración y Finanzas y/o Subgerente de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de la línea telefónica.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar.

Evento : **Falla de Equipo Firewall**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.1** FECHA: Versión:

4. PLAN DE PREVENCION

Descripción del evento

Este evento refiere a la falla del equipo de la Router donde se conecta el servicio de Internet, este equipo no es de propiedad de EMMSA , es del proveedor brinda el servicio de internet.

Hardware

Router de Internet

Objetivo

Mantener operativo el servicio de internet los 365 días del año y 24 horas.

Criticidad

Este evento se considera de Alto Impacto.

Entorno

Se puede producir durante la operatividad, afectando las transacciones y comunicaciones de EMMSA.

Personal Encargado

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

El Subgerente de Informática es responsable de hacer seguimiento y hacer de conocimiento sobre el funcionamiento del Router de Internet del Proveedor.

Condiciones de Prevención de Riesgo

- Informar al Gerente de Administración y Finanzas referente a las fallas que pudiera presentar el equipo router del proveedor de Servicio de Internet.
- Solicitar al proveedor mantenimiento preventivo de sus equipos por lo menos una vez al año depende del tiempo que se tenga contratado el servicio.

5. PLAN DE EJECUCIÓN

c. Eventos que activan la Contingencia

Falta de Internet en EMMSA.

d. Procesos Relacionados Antes del evento.

La falta del servicio de internet que imposibilita la comunicación electrónica y las transacciones que necesitan el servicio internet.

Personal que autoriza la contingencia

El Gerente de Administración y Finanzas y el Subgerente de Informática pueden activar la contingencia.

f. Descripción de las procedimientos después de activar la contingencia

- Informar al Gerente de Administración y Finanzas el problema presentado.
- Dar aviso a las áreas referente a la falta de internet ocasionado por el equipo router.
- Contactar con el proveedor del servicio de internet.

Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor realice el cambio del equipo router de Internet.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Subgerente de Informática se encargará de realizar las acciones de recuperación necesarias.

Descripción

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Se informará al Comité de Contingencia el Plan el problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Mecanismos de Comprobación

El Gerente de Administración y Finanzas y/o Subgerente de Informática presentará un informe explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Desactivación del Plan de Contingencia

El Gerente de Administración y Finanzas y/o Subgerente de Informática desactivará el Plan de Contingencia una vez que se cambie el Equipo Router de Internet.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar.

Evento : **Falla de Switch de la Sala de Telecomunicaciones**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.2** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla de los Switch de la Sala de Telecomunicaciones, estos Switch son los principales de todo EMMSA que permiten la conexión y a la red y a los recursos compartidos de los usuarios de EMMSA y el Sistema de Video Vigilancia.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados
- Correo Electrónico

Hardware

- Impresiones en Red
- Telefonía IP, Cámaras, Servidores, NVR.

Información

- Base de Datos de Sistemas.
- Archivos de Usuarios.

Objetivo

Asegurar la continuidad de las operaciones de los usuarios y del acceso a los recursos informáticos compartido de toda la empresa.

Criticidad

Este evento se considera como CRITICO.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios y los accesos a todas las conexiones a red y a internet de los usuarios de EMMSA.

Personal Encargado

El Subgerente de Informática encargará al responsable de las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Revisión periódica y mantenimiento preventivo de los switch de red del TELECOM.
- Contar con equipos de respaldo en caso de falla de los switch administrables.
  Tener copia de las configuraciones de los Switch.

2. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia las conexiones de los usuarios a internet u otro recurso compartido de red.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con las conexiones de red de los usuarios.

Personal que autoriza la contingencia

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Comunicar a los usuarios.
- Realizar pruebas de conexiones, reiniciar los switch de red.
- Reemplazo de equipos.

- Duración

La duración del evento no deberá ser mayor a DOS HORAS en caso de fallas de los equipos, se debe esperar la indicación del personal de informática para realizar las conexiones de red mediante los sistemas.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática luego de restaurar el correcto funcionamiento de la Switch coordinará con los usuarios área para reanudar las conexiones de los aplicativos y sistemas.

Descripción

Se informará al Subgerente de Informática las acciones realizadas y el procedimiento

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

correctivo para el funcionamiento de las conexiones de red.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias de los Switch de Red.

Evento : **Falla de Equipo Router de Internet**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.3** FECHA: Versión:

1. PLAN DE PREVENCIÓN

Descripción del evento

Este evento refiere a la falla del equipo de la Router donde se conecta el servicio de Internet, este equipo no es de propiedad de EMMSA , es del proveedor brinda el servicio de internet.

Hardware

Router de Internet

Objetivo

Mantener operativo el servicio de internet los 365 días del año y 24 horas.

Criticidad

Este evento se considera de Alto Impacto.

Entorno

Se puede producir durante la operatividad, afectando las transacciones y comunicaciones de EMMSA.

Personal Encargado

El Subgerente de Informática es responsable de hacer seguimiento y hacer de conocimiento sobre el funcionamiento del Router de Internet del Proveedor.

Condiciones de Prevención de Riesgo

- Informar al Gerente de Administración y Finanzas referente a las fallas que pudiera presentar el equipo router del proveedor de Servicio de Internet.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

- Solicitar al proveedor mantenimiento preventivo de sus equipos por lo menos una vez al año depende del tiempo que se tenga contratado el servicio.

2. PLAN DE EJECUCIÓN

d. Eventos que activan la Contingencia

Falta de Internet en EMMSA.

e. Procesos Relacionados Antes del evento.

La falta del servicio de internet que imposibilita la comunicación electrónica y las transacciones que necesitan el servicio internet.

Personal que autoriza la contingencia

El Gerente de Administración y Finanzas y el Subgerente de Informática pueden activar la contingencia.

g. Descripción de los procedimientos después de activar la contingencia.

- Informar al Gerente de Administración y Finanzas el problema presentado.
- Dar aviso a las áreas referente a la falta de internet ocasionado por el equipo router.
- Contactar con el proveedor del servicio de internet.

Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor realice el cambio del equipo router de Internet.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Subgerente de Informática se encargará de realizar las acciones de recuperación necesarias.

Descripción

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Se informará al Comité de Contingencia el Plan el problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso.

Mecanismos de Comprobación

El Gerente de Administración y Finanzas y/o Subgerente de Informática presentará un informe explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Desactivación del Plan de Contingencia

El Gerente de Administración y Finanzas y/o Subgerente de Informática desactivará el Plan de Contingencia una vez que se cambie el Equipo Router de Internet.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar.

Evento : **Falla de la Central Telefónica**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.4** FECHA: Versión:

1. PLAN DE PREVENCIÓN

Descripción del evento

Este evento refiere a la falla del equipo de la central telefónica que administra los anexos IPs para la comunicación de los usuarios de EMMSA.

Hardware

Central Telefónica

Software

Software de Central Telefónica

Objetivo

Restaurar o reparar el equipo de la central telefónica para la comunicación de la empresa.

Criticidad

Este evento se considera de Alto Impacto.

Entorno

Se puede producir durante la operatividad, afectando las comunicaciones de EMMSA.

Personal Encargado

El Subgerente de Informática es responsable del mantenimiento preventivo y/o solicitud de cambio de este equipo.

Condiciones de Prevención de Riesgo

- Informar al Gerente de Administración y Finanzas referente al mantenimiento preventivo de la central telefónica y/o adquisición de una nueva central telefónica de ser necesario.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

2. PLAN DE EJECUCIÓN

e. Eventos que activan la Contingencia

Falla de la Central Telefónica.

f. Procesos Relacionados Antes del evento.

La falta de comunicación en las instalaciones de EMMSA.

e. Personal que autoriza la contingencia

El Gerente de Administración y Finanzas y el Subgerente de Informática pueden activar la contingencia.

h. Descripción de las procedimientos después de activar la contingencia

- Informar al Gerente de Administración y Finanzas el problema presentado.
- Dar aviso a las áreas la falla de la central telefónica en especial a mesa de partes.
- Contactar con el proveedor de la central telefónica.

Duración

El tiempo máximo de duración de la contingencia dependerá del proveedor que repare la central telefónica.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Subgerente de Informática en coordinación con el Subgerente de Logística se encargará de realizar las acciones de recuperación necesarias.

Descripción

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Se informará al Comité de Contingencia el Plan el problema presentado y el procedimiento usado para atender el problema.

En función a esto, se tomarán las medidas preventivas del caso.

Mecanismos de Comprobación

El Gerente de Administración y Finanzas y/o Subgerente de Informática presentará un informe explicando que parte del Servicio u operación ha fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Desactivación del Plan de Contingencia

El Gerente de Administración y Finanzas y/o Subgerente de Informática desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de la central telefónica.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Falla de Switch de Red de 1er, 2do. y 3er Piso.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-3.5** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla de los Switch de Red de las Oficinas Administrativas que permiten la conexión y a la red y a los recursos compartidos de los usuarios de EMMSA.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados
- Correo Electrónico

Hardware

- Impresiones en Red
- Telefonía IP

Información

- Respaldo de Información de Archivos

Objetivo

Asegurar la continuidad de las operaciones de los usuarios y del acceso a los recursos informáticos compartidos.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios y los accesos a todos las conexiones a red y a internet de los usuarios de EMMSA.

Personal Encargado

El Subgerente de Informática encargará al responsable de las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Revisión periódica y mantenimiento preventivo de los switch de red.
- Contar con equipos de respaldo en caso de falla de los switch administrables.

  Tener copia de las configuraciones de los Switch.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

3. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia las conexiones de los usuarios a internet u otro recurso compartido de red.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con las conexiones de red de los usuarios.

Personal que autoriza la contingencia

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Comunicar a los usuarios.
- Realizar pruebas de conexiones, reiniciar los switch de red.
- Reemplazo de equipos.

- Duración

La duración del evento no deberá ser mayor a DOS HORAS en caso de fallas de los equipos, se debe esperar la indicación del personal de informática para realizar las conexiones de red mediante los sistemas.

4. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática luego de restaurar el correcto funcionamiento de la Switch coordinará con los usuarios área para reanudar las conexiones de los aplicativos y sistemas.

Descripción

Se informará al Subgerente de Informática las acciones realizadas y el procedimiento correctivo para el funcionamiento de los switch.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

necesarias de los Switch de Red.

Evento : **Falla del Hw o Sistema Operativo de los Servidores**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-4.1** FECHA: Versión:

1.PLAN DE PREVENCION

Descripción del evento

Ausencia del servicio principal para almacenar, procesar y proteger los datos, para acceso controlado y procesamiento de transacciones rápidos para cumplir con los requisitos de las aplicaciones consumidoras de datos más exigentes de EMMSA.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados

Hardware

- Servidores

Información

- Respaldo de Base de Datos
- Respaldo del Software Base

Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar los datos de las aplicaciones ejecutadas en los servidores centrales.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones de EMMSA.

Personal Encargado

El Subgerente de Informática encargará al responsable de la base de datos las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Revisión periódica de los logs de la BD para prevenir mal funcionamiento de la Base de Datos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción en la Institución. Se realizan copias de la información o de los registros con la finalidad de

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

asegurar la información mantenida en la base de datos.

- La copia de seguridad de la información es un proceso diario, en donde se busca asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos de acuerdo a requerimientos antes o después de un determinado proceso Anexo

  Copias de Respaldo.
- Mantener actualizado el software de gestión de BD.
- Realizar el mantenimiento preventivo anual de la BD.

Evento: Falla en las Base de Datos Oracle, SQL de los servidores.	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-5.1** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Ausencia del servicio principal para almacenar, procesar y proteger los datos, para acceso controlado y procesamiento de transacciones rápidos para cumplir con los requisitos de las aplicaciones consumidoras de datos más exigentes de EMMSA.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Software

- Aplicativos utilizados

Hardware

- Servidores

Información

- Respaldo de Base de Datos
- Respaldo del Software Base

Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados para restaurar los datos de las aplicaciones ejecutadas en los servidores centrales.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

a las operaciones de EMMSA.

Personal Encargado

El Subgerente de Informática encargará al responsable de la base de datos las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Revisión periódica de los logs de la BD para prevenir mal funcionamiento de la Base de Datos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción en la Institución. Se realizan copias de la información o de los registros con la finalidad de asegurar la información mantenida en la base de datos.
- La copia de seguridad de la información es un proceso diario, en donde se busca asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos de acuerdo a requerimientos antes o después de un determinado proceso Anexo

  Copias de Respaldo.
- Mantener actualizado el software de gestión de BD.
- Realizar el mantenimiento preventivo anual de la BD.

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

- Mensajes de error durante el almacenamiento o consultas de información.
- Lentitud en el acceso de información de la BD.
- Falla de conexiones a la BD.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con las conexiones de las aplicaciones a la BD.

Personal que autoriza la contingencia

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Comunicar a los usuarios para salgan de las aplicaciones con conexiones a la BD.
- Realizar SHUTDOWN a la Base de Datos.
- Activar la BD de respaldo.
- Probar las conexiones con las aplicaciones en producción.

- Duración

  La duración del evento no deberá ser mayor a DOS HORAS en caso se fallas de la BD.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Esperar la indicación del personal de informática para realizar conexiones con la BD.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática luego de restaurar el correcto funcionamiento de la BD coordinará con los usuarios área para reanudar las conexiones de los aplicativos y sistemas.

Descripción

Se informará al Subgerente de Informática las acciones realizadas y el procedimiento correctivo para el funcionamiento de la Base de Datos.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias en la BD. Se adjunta Anexo.

Evento : **Infección de Equipos por Falla o Vencimiento de Licencias ANTIVIRUS**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-6.2** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Virus informático es un programa de software que se propaga de un equipo a otro y que interfiere el funcionamiento del equipo. Además, Un virus informático puede dañar o eliminar los datos de un equipo.

Este evento incluye lo

te afectada o causa de la contingencia, los cuales se muestran a continuación:

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Hardware

Servidores

Estaciones de Trabajo

Software

Software Base

Aplicativos utilizados

Objetivo

Restaurar la operatividad de los equipos después de eliminar los virus o reinstalar las aplicaciones dañadas.

Criticidad

El nivel de éste evento es considerado CRITICO.

Entorno

Las estaciones de trabajo PCs, se encuentran instaladas en el GMML.

Personal Encargado

Subgerente de Informática del EMMSA es el responsable en la supervisión del correcto funcionamiento de las estaciones PCs

Condiciones de Prevención de Riesgo

- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación de quemadores de CD en estaciones de trabajo que no lo requieran.
- Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Aplicar filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con el uso de las aplicaciones en las estaciones de trabajo.

Personal que autoriza la contingencia

Subgerente de Informática

Técnico de Soporte

Descripción de las Actividades después de activar la contingencia

- Desconectar la estación infectada de la red.
- Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- Rastrear de ser necesario el origen de la infección (archivo infectado,
    - correo electrónico, etc.)
- Eliminar el agente causante de la infección.
- Remover el virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema:

  Formatear el equipo

  Personalizar la estación para el usuario
- Conectar la estación a la red.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

- Duración

  La duración del evento no deberá ser mayor a DOS HORAS en caso se confirme la presencia de un virus. Esperar la indicación del personal de soporte para reanudar el trabajo.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Técnico de Soporte de Sistemas, luego de restaurar el correcto funcionamiento de la estación de trabajo (PC), coordinará con el usuario responsable y/o Jefe del área para reanudar las labores de trabajo con el equipo.

Descripción

Se informará al Subgerente de Informática el tipo de virus encontrado y el procedimiento usado para removerlo.

En función a esto, se tomarán las medidas preventivas del caso enviando una alerta vía correo al personal de EMMSA

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Técnico de Soporte de Sistemas se desactivará el presente Plan.

Proceso de Actualización

El problema de infección presentado en la estación de trabajo, no debe detener la Aplicación de actualización de datos en las Aplicaciones de EMMSA.

Evento : **Falla de aplicativos propios de EMMSA.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-6.1** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción Del Evento

Es la ausencia de interacción entre el Software y el Hardware haciendo inoperativa la máquina, es decir, el Software no envía instrucciones al Hardware imposibilitando su funcionamiento.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA, que por su

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

Software

- Software base
- Software base de datos
- Aplicativos utilizados por el EMMSA

Hardware

- Servidores

Información

- Respaldo de base de datos
- Respaldo de las aplicaciones utilizadas
- Respaldo De Software Base

Objetivo

Mantener operativo los servidores de producción donde se ejecutan las aplicaciones.

Criticidad

El nivel de este evento es considerado crítico.

Entorno

Los servidores de aplicaciones están situados en la Sala de Telecomunicaciones.

Personal Encargado

Subgerente de Informática de EMMSA es el responsable de asegurar el correcto funcionamiento de los servidores durante los servicios. Se coordinarán las acciones necesarias para restablecer el servicio en caso se produzca el evento.

También será el encargado de coordinar las acciones necesarias con l personal de las áreas usuarias, para asegurar un servicio continuo de los servidores y sus aplicaciones, de tal forma que no afecten el servicio brindado especialmente en GARITAS.

Condiciones de Prevención de Riesgo

Tomar las siguientes acciones preventivas que debe implementar la Subgerencia de Informática para asegurar el servicio de las aplicaciones:

- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con mantenimiento preventivo para dichos equipos.
- Contar con los backups de información necesarios para restablecer las aplicaciones Anexo: Copias de Respaldo.
- Contar con backups de las aplicaciones y de las bases de datos Anexo
- Almacenar en un lugar seguro los backups referidos a aplicaciones y datos. Se

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

recomienda el almacenamiento De Los Backups en un lugar externo fuera de las instalaciones de EMMSA

2. PLAN DE EJECUCIÓN

Eventos que Activan La Contingencia

- Falla de Acceso a Aplicaciones.
- Mensaje Pérdida de Conexión a La BD.

Procesos Relacionados Antes Del Evento.

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores de EMMSA

Personal que autoriza la contingencia Subgerente de

Informática

Descripción de Las Actividades Después de Activar La Contingencia Remitirse a los Procedimientos de recuperación de sistemas.

Duración

La duración del evento estará en función de la complejidad del problema encontrado.

Esperar la indicación del jefe de Informática de IMARPE para reanudar la operación normal con las aplicaciones.

3. PLAN DE RECUPERACIÓN

. Personal encargado

El Subgerente de Informática luego de verificar la corrección del problema de acceso a los servidores, coordinará con los Usuarios de las áreas para la reanudación de los trabajos operativos con las aplicaciones (SAFIM,TRAMITE, ETC).

Descripción

Se informará a la Alta Dirección la causa que motivó la paralización del servicio.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la coordinación ejecutora del plan para su revisión.

Desactivación del plan de contingencia

Con el aviso del Subgerente de Informática se desactivará el presente plan.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Proceso de actualización

En caso existiese información pendiente de actualización, debido a la falla de los sistemas principales se coordinará con los Gerentes para iniciar las labores de actualización de los sistemas.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Suspensión de Servicio de Correo Electrónico GMAIL**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-7.1** FECHA: Versión:

1.PLAN DE PREVENCION

Descripción Del Evento

Es la ausencia del servicio de correo electrónico de EMMSA, este evento no permite el medio de comunicación de los usuarios de Emmsa para su trabajo diario.

Software

- Accesos a aplicativos de cuentas de GMAIL.

Información

- Bandeja de Entrada de Usuarios

Objetivo

Mantener operativo el servicio de correo corporativo.

Criticidad

El nivel de este evento es considerado crítico.

Entorno

El servicio de correo se encuentra en la nube.

Personal Encargado

El Subgerente de Informática de EMMSA es el responsable de asegurar que el servicio de correos corporativos sea continuo.

Condiciones de Prevención de Riesgo

Tomar las siguientes acciones preventivas que debe implementar la Subgerencia de Informática para asegurar el servicio de correos:

- Coordinar con la Subgerencia de Logística para la continuidad del servicio. .
- Contar habilitado el servicio de Internet.

2. Plan de Ejecución

Eventos que Activan La Contingencia

- Servicio no habilitado.

Procesos Relacionados Antes Del Evento.

Cualquier proceso relacionado con el uso de correos electrónicos por parte de los usuarios de EMMSA.

Personal que autoriza la contingencia Subgerente

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

de Informática.

Descripción de Las Actividades Después de Activar La Contingencia

Remitirse a los Procedimientos para la activación del servicio en coordinación con la Subgerencia de Logística.

Duración

La duración del evento estará en función a la habilitación del pago del servicio de correos electrónicos.

3. Plan de Recuperación

. Personal encargado

El Subgerente de Informática luego de verificar la habilitación del servicio coordinará con los Usuarios de las áreas para la reanudación de las comunicaciones internas.

Descripción

Se informará a la Alta Dirección la causa que motivó la paralización del servicio. En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá a la coordinación ejecutora del plan para su revisión.

Desactivación del plan de contingencia

Con el aviso del Subgerente de Informática se desactivará el presente plan.

Proceso de actualización

En caso de existir información pendiente de actualización, debido al corte del servicio del medio de comunicación corporativo se coordinará con los Gerentes para que los usuarios puedan ingresar a sus correos electrónicos.

Evento : **Sustracción o Robo de Información**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-8.1** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del Evento:

La sustracción o **robo de información** es un delito informático, consistente en la sustracción en este caso de datos correspondientes a la empresa.Este evento incluye los siguientes elementos mínimos identificados por EMMSA, los mismos

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUBGERENTE EMMSA

que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Información

- La información generada y administrada por los sistemas informáticos en la empresa.

Recursos Humanos

• Personal de Subgerencia de Informática y la Subgerencia de Seguridad debidamente entrenado para afrontar el evento.

Objetivo

Establecer las acciones que se ejecutaran ante un robo de información a fin de minimizar las consecuencias y la integridad de la información correspondiente a EMMSA.

Criticidad

EMMSA determina que el presente evento tiene un nivel de Alto impacto en el Servicio.

Entorno

Este evento se puede dar en las oficinas de las Gerencias y Subgerencias de EMMSA.

Personal Encargado

El Subgerente de Informática y todo el personal de la empresa es quien debe dar cumplimiento a lo descrito en las Condiciones de Prevención de Riesgo del presente Plan.

Condiciones de Prevención de Riesgo

- Aplicar las políticas de seguridad informática establecidas en las directivas por la Subgerencia de Informática.
- Establecer seguridad física en todos los ambientes del área de informática y/o otras áreas donde se encuentren equipos informáticos.

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

La Contingencia se activará al ocurrir la detección de la sustracción de información.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

Procesos Relacionados antes del evento.

- Identificar los equipos y las áreas de donde han sido sustraídos los datos.
- Identificar los usuarios que utilizaban estos equipos.
- Informe de los usuarios a la Subgerencia de Seguridad.
- Solicitar los videos de seguridad de las instalaciones cerca al evento ocurrido a la
  Subgerencia de Seguridad.
- Tener número de teléfono del personal responsable del personal de la Subgerencia de Informática y del equipo de Contingencia de EMMSA.

Personal que autoriza la contingencia.

El Gerente de Administración y Finanzas o el Subgerente de Informática pueden activar la contingencia.

Descripción de las actividades después de activar la contingencia.

- Verificar los accesos a los sistemas y equipos vulnerados.
- Comunicar al personal responsable de EMMSA.
- En todo momento se coordinará con el Comité de Contingencia y
  La Subgerencia de Seguridad, para las acciones que deban ser efectuadas por ellos.

Luego de haber superado la sustracción de información , se deberán realizar las siguientes actividades:

- Mejorar las políticas de seguridad.

La Coordinación Ejecutora del Plan de Contingencias deberá coordinar con la Alta Dirección de EMMSA en caso se requiera las denuncias respectivas en coordinación con la Subgerencia de Seguridad.

g. Duración

La duración de la contingencia dependerá del tiempo y el impacto de la información sustraída.

SUB-GERENCIA DE INFORMATICA V°B° J. RAMIREZ SUB-GERENTE EMMSA

Evento	Entidad Responsable Involucrada	SI-PC-9.1
Ausencia imprevista del Personal Informático	**EMMSA**	FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Ausencias del personal de Soporte Técnico relevante (enfermedad, renuncias, ceses), en toma decisiones claves que garantice el normal funcionamiento de servidores y redes de la institución.

Este evento incluye los siguientes elementos mínimos identificados por el EMMSA , los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Recursos Humanos

Personal

b. Objetivo

Asegurar la continuidad del Servicio Informático de EMMSA.

c. Criticidad

EMMSA determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno

Este evento se puede dar en las instalaciones de la Alta Dirección, Gerencias y Subgerencias del Gran Mercado Mayorista de Lima.

e. Personal Encargado

El Gerente de Administración y Finanzas y/o el Subgerente de Informática es quién debe disponer se cumplan las Condiciones de Previsión de Riesgo del presente Plan.

f. Condiciones de Prevención de Riesgo

La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales, por lo que se considera lo siguiente:

- Como primera prevención, el Subgerente de Informática, se asegurará en capacitar a los analistas de sistemas del área de soporte técnico con el fin que cumpla el perfil, conocimiento y capacidad para reemplazar la ausencia ante la presencia de este evento.
- Como segunda prevención, el Subgerente de Informática se asegurara en

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

tener como mínimo a dos profesionales técnicos en el área de soporte técnico y un asistente.

- Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labores.
- Para el control del personal se cuenta con un software de control de asistencia, de donde se proveerá información al el Subgerente de Informática, para que tome las acciones preventivas correspondientes.

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

Reporte de inasistencia del personal de Soporte Técnico: administrador de la Red, administrador de la Base de Datos, helpdesk, etc.

El proceso de contingencia se activa durante las DOS (02) HORAS iniciales del día.

Procesos Relacionados Antes del evento.

Se podría dar por:

- Conocimiento del el Subgerente de Informática por parte del reporte de inasistencia del Sistema de Control de Asistencia.
- Conocimiento del el Subgerente de Informática por comunicación telefónica por parte del personal de Soporte Técnico ausente o algún familiar.

Personal que autoriza la contingencia es el

Subgerente de Informática.

Descripción de las Actividades después de activar la contingencia

- Confirmado la inasistencia del personal de soporte Técnico, el Subgerente de Informática asignará la responsabilidad al Asistente del área de soporte técnico capacitado para reemplazar en las funciones que el personal titular de soporte técnico poseía.
- El Subgerente de Informática de Informática solicitará al Gerente de Administración y Finanzas, el reemplazo del personal.

Duración

Máximo OCHO (08) horas. El fin del presente evento es la presencia del reemplazo que asume la responsabilidad; hasta que se confirme la presencia del personal de Soporte Técnico en caso de renuncia u otras por fuerza mayor.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

3. PLAN DE RECUPERACIÓN

Personal Encargado

El personal encargado del Plan de Recuperación es el Subgerente de Informática, cuyo rol principal es asegurar el normal funcionamiento del Servicio Informático.

Descripción

- Regularización en los servicios pendiente durante la ausencia.
- Revisión de los servicios atendidos si fuera el caso.
- Definir los ajustes para asegurar rápida y mejora en la acción y prevención del presente evento.

Mecanismos de Comprobación

El Subgerente de Informática presentará un informe al Comité ejecutor del Plan explicando que parte del Servicio Informático ha sido afectado y cual son las acciones tomadas.

Desactivación del Plan de Contingencia

El Subgerente de Informática desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan.

Proceso de Actualización

En base al informe presentado por el Subgerente de Informática y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Falta de idoneidad del personal respecto a la Información de la Base de Datos**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-9.2** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

La falta de las condiciones necesarias para desempeñar la función de garantizar la discreción y profesionalismo en el manejo de la información, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Recursos Humanos

Personal

c. Objetivo

Asegurar la discreción de la información almacenada y administrada en la Base de Datos.

d. Criticidad

EMMSA determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

e. Entorno

Este evento se puede dar en todo EMMSA.

f. Personal Encargado

El Gerente de Administración y Finanzas y/o el Subgerente de Informática es quién debe disponer se cumplan las Condiciones de Previsión de Riesgo del presente Plan.

f. Condiciones de Prevención de Riesgo

La existencia del presente evento se puede dar en cualquier momento, dependiendo de las circunstancias personales, por lo que se considera lo siguiente:

- Como primera prevención, el Subgerente de Informática deberá monitorear los backups de base de datos.
- Como segunda prevención, el Subgerente de Informática se asegurara en tener informes escritos de las actividades realizadas por el administrador de la base de datos.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

Confirmación o visualización de la información de la empresa en otros medios electrónicos.

Procesos Relacionados Antes del evento.

Se podría dar por:

- Conocimiento del Subgerente de Informática por monitoreo de actividades.

Personal que autoriza la contingencia es el

Subgerente de Informática.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El personal encargado del Plan de Recuperación es el Subgerente de Informática, cuyo rol principal es asegurar que la persona que no administre correctamente la información deje de operar o accesar a esta.

Descripción

- Monitorear los logs de las base de datos.

Mecanismos de Comprobación

El Subgerente de Informática presentará un informe al Comité ejecutor del Plan explicando que parte del Servicio Informático ha sido afectado y cual son las acciones tomadas.

Desactivación del Plan de Contingencia

El Subgerente de Informática desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en la Descripción del presente Plan de Recuperación, mediante una comunicación electrónica a la Coordinación Ejecutora del Plan y con la cooperación de la Subgerencia de Recursos Humanos o Subgerencia de Logística.

Proceso de Actualización

En base al informe presentado por el Subgerente de Informática y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Fallas de Cámaras Domos o Fijas**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-10.1** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla de las Camaras Domos o Fijas del Sistema de Video Vigilancia de EMMSA.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Hardware

- Cámaras
- Pcs de Monitoreos

Objetivo

Asegurar la continuidad de las operaciones de los usuarios de la Subgerencia de Seguridad.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios de EMMSA.

Personal Encargado

El Subgerente de Informática encargará al responsable de las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Contratar revisión y mantenimiento preventivo de las cámaras.
- Contar con cámaras de reemplazo.

2. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia es la alerta de la Subgerencia de Seguridad que no visualizan las zonas por cámaras.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con el monitoreo de las cámaras.

Personal que autoriza la contingencia

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Comunicar al personal de la Subgerencia de Seguridad y Gerencia de Operaciones.
- Contactar con el Proveedor de Cámaras.

Duración

La duración del evento no deberá ser mayor a SEIS HORAS en caso de fallas de los equipos, se debe esperar la indicación del personal de informática y del proveedor.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática y el Proveedor del Servicio de Mantenimiento luego de restaurar el correcto funcionamiento de las cámaras coordinará con los usuarios área para reanudar las visualizaciones.

Descripción

Se informará al Subgerente de Seguridad las acciones realizadas y el procedimiento correctivo para el funcionamiento de las camaras.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias de las cámaras domos y fijas.

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Fallas de Grabación de los NVRs.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-10.2** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla del NVRs de Grabación del Sistema de Video Vigilancia de EMMSA.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Hardware

- Grabador NVRs

Objetivo

Asegurar la continuidad de las operaciones de los usuarios de la Subgerencia de Seguridad y contar con las ocurrencias almacenadas.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios de EMMSA.

Personal Encargado

El Subgerente de Informática encargará al responsable de las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Contratar revisión y mantenimiento preventivo del NVR.

2. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia es la alerta de la Subgerencia de Seguridad cuando solicitan videos de fechas que no se encuentran registradas o mensajes de error en los NVRs.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con el monitoreo de los NVRs..

Personal que autoriza la contingencia

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Comunicar al personal de la Subgerencia de Seguridad y Gerencia de Operaciones.
- Contactar con el Proveedor del Sistema de Video Vigilancia.

Duración

La duración del evento no deberá ser mayor a SEIS HORAS en caso de fallas de los equipos, se debe esperar la indicación del personal de informática y del proveedor.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática y el Proveedor del Servicio de Mantenimiento luego de restaurar el correcto funcionamiento de los NVRs coordinará con los usuarios área para reanudar las grabaciones.

Descripción

Se informará al Subgerente de Seguridad las acciones realizadas y el procedimiento correctivo para el funcionamiento de los NVRs.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias para el buen funcionamiento de los NVRs.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Fallas de Equipos de Monitoreo**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-10.3** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla de los monitores de la Sala de Video Vigilancia de EMMSA.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Hardware

- Monitores

Objetivo

Asegurar la continuidad de las operaciones de los usuarios de la Subgerencia de Seguridad y permitir el monitoreo constante del GMML.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios de EMMSA y GMML.

Personal Encargado

El Subgerente de Informática se encargará de las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Contratar revisión y mantenimiento de los Monitores del Sistema de Video Vigilancia.

2. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia es la alerta de la Subgerencia de Seguridad cuando no se puedan visualizar en la sala de video vigilancia.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con el monitoreo de las cámaras.

Personal que autoriza la contingencia

Subgerente de Informática

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Descripción de las Actividades después de activar la contingencia

- Comunicar al personal de la Subgerencia de Seguridad y Gerencia de Operaciones.
- Contactar con el Proveedor del Sistema de Video Vigilancia.

Duración

La duración del evento no deberá ser mayor a 3 HORAS en caso de fallas de los equipos, se debe esperar la indicación del personal de informática y del proveedor.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática y el Proveedor del Servicio de Mantenimiento luego de restaurar el correcto funcionamiento de los monitores coordinará con los usuarios área para reanudar las visualizaciones.

Descripción

Se informará al Subgerente de Seguridad las acciones realizadas y el procedimiento correctivo para el funcionamiento de los monitores de la sala.
En función a esto, se tomarán las medidas preventivas.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias para el buen funcionamiento de los Monitores del Sistema de Video Vigilancia.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Evento : **Falla de Computadoras, Impresoras, Escáner, Marcadores de Huella.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.1** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla de Equipos de uso constante para los usuarios de EMMSA.

Este evento incluye los siguientes elementos mínimos identificados los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

Computadoras, Impresoras,

Escáner, Marcadores de Huella

Software

Sistema Operativo

Objetivo

Restaurar la operatividad de los equipos.

Criticidad

El nivel de éste evento es considerado de Impacto Moderado.

Entorno

Las estaciones de trabajo PCs, se encuentran instaladas en el GMML.

Personal Encargado

Subgerente de Informática del EMMSA es el responsable en la supervisión del correcto funcionamiento de las estaciones PCs

Condiciones de Prevención de Riesgo

- Mantenimiento Preventivo y Mantenimiento Correctivo Oportuno.

2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

- Mensajes de error.
- Falla general en el equipo (sistema operativo, aplicaciones).

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con el uso de las aplicaciones en las estaciones de trabajo.

Personal que autoriza la contingencia

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Subgerente de Informática

Técnico de Soporte

Descripción de las Actividades después de activar la contingencia

- Desconectar el equipo.
- Verificar si las fallas son de Hw y Software.
- Si es Software se reinstala el Sistema Operativo.
- Si Hardware se derivara a Mantenimiento de Equipos – Subgerencia de Logística.
- En caso no solucionarse el problema:

  Formatear el equipo

  Derivar a un proveedor externo.

- Duración

La duración del evento no deberá ser mayor a 4 HORAS . Esperar la indicación del personal de soporte para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Técnico de Soporte de Sistemas, luego de restaurar el correcto funcionamiento de la estación de trabajo u otro equipo , coordinará con el usuario responsable y/o Jefe del área para reanudar las labores de trabajo con el equipo.

Descripción

Se informará al Subgerente de Informática las fallas del equipo y el procedimiento correctivo.

En función a esto, se tomarán las medidas preventivas en coordinación con Mantenimiento de Equipos.

Se les brindara otro equipo de contar con ello.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Técnico de Soporte de Sistemas se desactivará el presente Plan.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Proceso de Actualización

El problema de presentado por los equipos, no debe detener la operatividad de los usuarios.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones de los equipos.

Evento : **Falla de Aire Acondicionado del TELECOM.**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.2** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla de los Equipos de Aire acondicionado en la Sala de Servidores, este ambiente siempre tiene que estar con una temperatura adecuada para el funcionamiento de los servidores y amplíen su vida útil.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Hardware

- Servidores
- Equipos TELECOM

Información

- Base de Datos EMMSA.

Objetivo

Asegurar la continuidad de las operaciones de los usuarios y del acceso a los recursos informáticos compartidos.

Criticidad

Este evento se considera como CRITICO.

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios y los accesos a todas las conexiones a red y a internet de los usuarios y otros

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

aplicativos de EMMSA.

Personal Encargado

El Subgerente de Informática encargará al responsable de las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Contratar anualmente el mantenimiento preventivo en coordinación con la Subgerencia de Logística.

2. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia
  La temperatura del ambiente del TELECOM.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con el ambiente de la sala de servidores.

Personal que autoriza la contingencia

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Contactar con el proveedor para el mantenimiento.
- Colocar ventiladoras temporalmente hasta q se repare el Aire Acondicionado.
- Duración

La duración del evento no deberá ser mayor a SEIS HORAS en caso de fallas de los equipos.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática luego de restaurar el correcto funcionamiento del aire acondicionado reanudara las operaciones.

Descripción

El Subgerente de Informática las acciones realizadas y el procedimiento correctivo para el funcionamiento del aire acondicionado.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias para el buen funcionamiento del aire acondicionado.

Evento : **Falla de UPS Telecom y otros**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.3** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla del Ups de la Sala de Servidores permite regular la corriente que llega a los servidores y ante un corte de energía permite que sigan trabajando los equipos hasta que se active el grupo electrógeno.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Hardware

- Servidores
- Equipos TELECOM

Información

- Base de Datos EMMSA.

Objetivo

Asegurar la continuidad de las operaciones de los usuarios y del acceso a los recursos informáticos compartidos.

Criticidad

Este evento se considera como Gran Impacto.

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios ya que los equipos ante un corte de luz pueden sufrir daños si no se contaría con los Ups.

Personal Encargado

El Subgerente de Informática encargará de las acciones correspondientes.

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Condiciones de Prevención de Riesgo

- Contratar anualmente el mantenimiento preventivo en coordinación con la Subgerencia de Logistica.

2. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia
  Los cortes de energía y el funcionamiento del UPS del TELECOM.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado con que desestabilice la corriente de energía de la sala de servidores.

Personal que autoriza la contingencia

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Contactar con el proveedor para el mantenimiento.
- Coordinar con Mantenimiento de Equipos para su monitoreo.

- Duración

La duración del evento no deberá ser mayor a 2 HORAS en caso de fallas de los equipos.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática luego de restaurar el correcto funcionamiento del UPS reanudara las operaciones.

Descripción

El Subgerente de Informática las acciones realizadas y el procedimiento correctivo para el funcionamiento del UPS.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias para el buen funcionamiento del UPS

Evento : **Falla de Grupo Electrógeno**	Entidad Responsable Involucrada: **EMMSA**	**SI-PC-11.4** FECHA: Versión:

1. PLAN DE PREVENCION

Descripción del evento

Falla del Grupo Electrógeno no permitirá la continuidad del servicio de Garitas ya que no alimentaria de corriente a los servidores de la Sala de Telecomunicaciones dejando inoperativo el ingreso del GMML.

Este evento incluye los siguientes elementos mínimos identificados por EMMSA , que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Hardware

- Servidores
- Equipos TELECOM

Información

- Sistemas Informáticos , Base de Datos EMMSA.

Objetivo

Asegurar la continuidad de las operaciones de los usuarios y del acceso a los recursos informáticos.

Criticidad

Este evento se considera como Gran Impacto.

Entorno

Se puede producir durante el servicio, afectando a todos los usuarios y en especial a las garitas.

Personal Encargado

El Subgerente de Informática y el Subgerente de Logistica se encargará de las acciones correspondientes.

Condiciones de Prevención de Riesgo

- Contratar anualmente el mantenimiento preventivo en coordinación con la Subgerencia de Logística.

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

2. PLAN DE EJECUCIÓN

- Eventos que activan la Contingencia
  Los cortes de energía y el funcionamiento del Grupo Electrógeno conectado al TELECOM.

Procesos Relacionados Antes del evento.

Cualquier proceso relacionado que no permita la activación del grupo electrógeno.

Personal que autoriza la contingencia

Subgerente de Informática

Descripción de las Actividades después de activar la contingencia

- Contactar con el proveedor para el mantenimiento.
- Coordinar con Mantenimiento de Equipos para su monitoreo.
- Duración
  La duración del evento no deberá ser mayor a 2 HORAS en caso de fallas de los equipos.

3. PLAN DE RECUPERACIÓN

Personal Encargado

El Personal de Informática y el Personal de Mantenimiento luego de restaurar el correcto funcionamiento del Grupo Electrógeno.

Descripción

El Subgerente de Informática las acciones realizadas y el procedimiento correctivo para el funcionamiento del Grupo Electrógeno.

En función a esto, se tomarán las medidas preventivas.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

las correcciones necesarias para el buen funcionamiento del Grupo Electrógeno en función a esto, se tomarán las medidas preventivas.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

Mecanismos de Comprobación

Se llenará el formato de ocurrencia de eventos y se remitirá al comité de Contingencia.

Desactivación del Plan de Contingencia

Con el aviso del Subgerente de Sistemas se desactivará el presente Plan.

Proceso de Actualización

En base al informe determinarán las acciones de prevención a tomar para las correcciones necesarias para el buen funcionamiento del grupo electrógeno.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

12. Identificar impactos de la caída y tiempos aceptables de caída.

IDENTIFICAR IMPACTOS DE LA CAÍDA Y TIEMPOS ACEPTABLES DE CAÍDA		
Recursos	**Impacto de la caída**	**Tiempo de caída aceptable**
Sistema SAFIM	• No se pueden registrar camiones, pesaje y distribución de carga. • No se pueden ingresar a los módulos de contabilidad, tesorería, presupuesto, cobranzas, logística, planillas, etc.	2 horas
Sistema de Tramite	• No se pueden generar memos, cartas oficios, ni registrar documentos.	3 horas
Internet	• No se puede enviar correos electrónicos. • No se pueden acceder a sistemas online SUNAT, SEACE, etc.	3 horas
Central Telefónica	• No se pueden realizar ni recibir llamadas	2 horas
Sistema SISCOP	• No se puede realizar el control de asistencia del personal.	3 horas
PDT	• No se pueden realizar declaraciones tributarias.	3 horas
Sistema de Inscripción de Concesionarios	• No permite la creación, actualización o a de los distintos registros de Concesionarios (Adjudicados y/o Temporales). • No permite visualización de data histórica de Concesionarios Adjudicados.	3 horas
Sistema de CCTV	• No permite la grabación de videos de seguridad ante cualquier incidente. • No permite el permanente monitoreo de seguridad en las instalaciones del GMML.	2 horas

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

13. Observaciones

La contingencia no debe extenderse a más de un día salvo casos extremos, paralelamente a los procedimientos de recuperación y como parte de ellos; se debe contactar con los proveedores de los equipos y recursos necesarios para asegurar la continuidad de las operaciones en condiciones normales.

14. Conclusiones

- El presente Plan de contingencia, tiene como objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.
- Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Evaluación de riesgos, Asignación de prioridades a las aplicaciones, Establecimiento de los requerimientos de recuperación, Elaboración de la documentación, Verificación e implementación del plan, Distribución y mantenimiento del plan.
- El Plan de Contingencia es una herramienta para EMMSA, que permitirá desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones. Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.
- El plan de Contingencia de la Empresa Municipal de Mercados está sujeto a la infraestructura física y las funciones que se realiza dentro del espacio asignado para la Sala de Servidores en el Gran Mercado Mayorista de Lima.
- Lo único que realmente permitirá a la Empresa Municipal de Mercados reaccionar adecuadamente ante procesos críticos, es la prueba y mantenimiento de un Plan de Contingencia.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

15. Recomendaciones

- Programar las actividades propuestas en el presente Plan de Contingencias.
- Hacer de conocimiento general el contenido del presente Plan de Contingencias con la finalidad de instruir adecuadamente al personal de la Empresa Municipal de Mercados.
- Adicionalmente al plan de contingencias se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.
- Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de Institución

Anexos

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

Anexo: Plan de Recuperación
Lista de Proveedores

PROVEEDOR	RAZON SOCIAL	CONTACTO	CORREO	TELEFONOS
GUPTA	BSI REPRESENTACIONES Y SERVICIOS S.A.C.	ALEXANDER CORONEL	acoronel@bsiconsulting.pe Alexander.bsir@gmail.com	Teléfono: 4750036
FACTURACION ELECTRONICA	INDIGITAL & EDICOM S.A.C.	MAURICIO PAREDES	mparedes@indigitalsolutions.com	Teléfono: 6535906 Celular: 956245373
CAMARAS VIDEO VIGILANCIA	UNTIVEROS,BOZA & ALEJOS TECHNOLOGIES S.A.C.//UBATEC S.A.C.	HERMOGENES UNTIVEROS	huntiveros@ubatec.net	Telefono: 531 – 9218 Cel: 99654 – 4455 RPM: #246116 RPC: 980584843
FORTIGATE	GRID SOLUTIONS S.R.L	FERNANDO CHACALTANA	jchacaltana@gridsolutionsperu.com	Celular:943007956 Celular:93936598
ESET ENDPOINT SECURITY	VILSOFT S.A.C.	ISABEL MENDOZA	isabel.mendoza@vilsoft.com.pe	Teléfono: (511) 2745309
SERVICIOS DE CUSTODIA Y TRASLADO DE MEDIOS MAGNETICOS	AIRON MOUNTAIN	JEAN PIERRE ANIENTO	Jean.aniento@ironmountain.com.pe	Teléfono: 7114000 Celular:981059703
GUPTA	BSI REPRESENTACIONES Y SERVICIOS S.A.C.	ALEXANDER CORONEL	acoronel@bsiconsulting.pe Alexander.bsir@gmail.com	Teléfono: 4750036
FACTURACION ELECTRONICA	INDIGITAL & EDICOM S.A.C.	MAURICIO PAREDES	mparedes@indigitalsolutions.com	Teléfono: 6535906 Celular: 956245373
CAMARAS VIDEO VIGILANCIA	UNTIVEROS,BOZA & ALEJOS TECHNOLOGIES S.A.C.//UBATEC S.A.C.	HERMOGENES UNTIVEROS	huntiveros@ubatec.net	Telefono: 531 – 9218 Cel: 99654 – 4455 RPM: #246116 RPC: 980584843
FORTIGATE	GRID SOLUTIONS S.R.L	FERNANDO CHACALTANA	jchacaltana@gridsolutionsperu.com	Celular:943007956 Celular:93936598

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

PROVEEDOR	RAZON SOCIAL	CONTACTO	CORREO	TELEFONO
TELEFONICA CLARO	AMERICA MOVIL PERU S.A.C.	DAVID ALEXIS GIOVE RAMOS	david.giove@claro.com.pe	Teléfono: 6131000 Celular: 982151696
TELEFONICA DEL PERU	TELEFONICA DEL PERU S.A.A	ABDEL RAMIREZ	Abdel.ramirez@telefonica.com	Teléfono: 2106245
SERVICIO DE CORREOS ELECTRONICOS	NOVALTEK GROUP	MARCO ANTONIO DE LA TORRE UGARTE	soporte@ngsac.pe	Teléfono:6404100 RPM: 987582536
HOSTING Y DOMINIO	WHODP COMUNICACIÓN VISUAL	EDGAR VARGAS	evargas@whodp.com	Celular:954717488
MANTENIMIENTO PREVENTIVO DE VIDEO VIGILANCIA	JOABH TELCOM	DANI VELASQUEZ	dani.velsquez@ joabh telcom.com	Celular:990012430
MANTENIMIENTO DE LA CENTRAL TELEFONICA	MR TECNYSOL S.R.L.	INES GUARDIA SOLA	ventas@ mrtecnysol.com	Teléfono:2269381 Celular:990396044
AIRE ACONDICIONADO	MULTIMIX COMPANY	VICTOR PACHECO	Multicompany2@gmail.com	Teléfono:3027207//2439602 RPM: #996930450 RPC: 992120193

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

Anexo: Plan de Recuperación
ROLES CRÍTICOS SAFIM

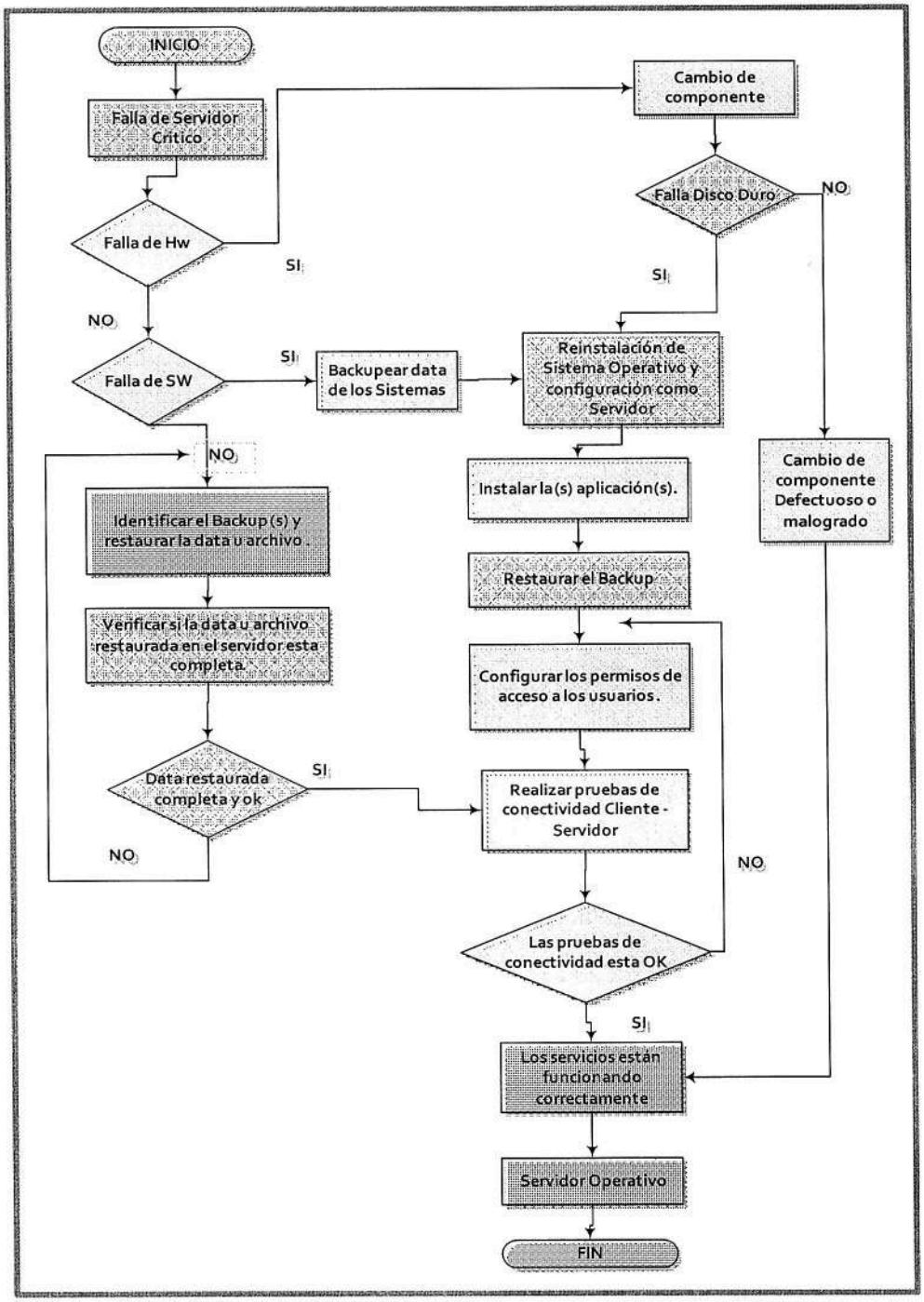
ACTIVIDADES POR USUARIOS	
Especialista en Presupuesto y Estadística	• Operar el sistema computarizado de presupuesto. • Registrar y procesar la información estadística relacionada a su área.
Asistente en Logística	• Consolidar el cuadro de necesidades de bienes y servicios. • Plan Anual de Adquisiciones. • Elaborar las bases administrativas, de acuerdo a las políticas y normas de adquisiciones y contrataciones. • Revisar la ficha técnica y los términos de referencia (TDR). • Elaborar orden de compra o servicio. • Supervisar registro, recepción, almacenamiento de documentación base.
Asistente de Control Patrimonial y Almacén	• Recepcionar y registrar los materiales y bienes diversos que adquiere la empresa, tramitando la conformidad en las guías de remisión. • Mantener organizada el área física del almacén para racional ingreso, ubicación y custodia de bienes. • Realizar seguimiento de las órdenes de compra pendientes de atención • Despachar y registrar los materiales y bienes diversos del almacén. • Codificar, etiquetar, registrar y controlar los bienes patrimoniales de la empresa.
Especialista de Personal	• Registrar y controlar la asistencia y permanencia del personal y elaborar y proponer el rol de vacaciones. • Elabora la planilla mensual del personal. • Generación de información base para el pago de impuestos referentes a pago de sueldos.
Asistente en Tesorería	• Comprobar el ingreso por todo concepto y control del manejo de fondos para pagos en efectivo. • Recibir, registrar y controlar los fondos. • Operar correctamente las opciones de los módulos de tesorería.
Especialista en Contabilidad	• Registrar en el Sistema el tipo de cambio (Nuevos Soles por US$). • Emisión de notas contables. • Provisiones y asientos contables • Elaborar los E.E.F.F. y libros contables. • Operar correctamente los módulos de contabilidad.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Personal de Garitas	• Recaudar los ingresos económicos en las garitas, emitiendo el comprobante respectivo. • Verificar y registrar en el SAFIM, la información sobre los productos que ingresen al mercado por las Garitas y al procedencia de los mismos.. • Realizar la liquidación en el libro de Garitas de la documentación utilizada y del dinero recaudado durante el servicio.
Especialista en Informática	• Cautelar por la seguridad e integridad de la Base de datos • Establecer mecanismo y procedimientos para un correcto resguardo (BACKUP) de la información. • Organizar, ejecutar y controlar las actividades de informática y comunicaciones. • Administración de los servidores instalados.
Asistente de Gerencia de Administración y Finanzas	• Recibir y registrar el flujo documentario. • Elaborar documentos con indicaciones precisas del gerente. • Elaborar la agenda de actividades de la Gerencia de Administración y Finanzas y mantener informado al gerente.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Anexo: Plan de Recuperación
Falla del Hw o Sistema Operativo de los Servidores



SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

Anexo: Plan de Recuperación
Falla del Hw o Sistema Operativo de los Servidores

DESCRIPCION DEL PROCEDIMIENTO		
PROCEDIMIENTO: VERIFICACION DE FALLAS DE LOS SERVIDORES DEL GMML.		
AREA: DEPARTAMENTO DE INFORMATICA		
RESPONSABLE	**ACT. NUMERO**	**DESCRIPCION DE ACTIVIDADES**
SUBGERENCIA DE INFORMATICA	**VERIFICACION DEL HARDWARE**	
	1	Se verifica si enciende el servidor
	2	Si el servidor no enciende se procede al cambio de componentes que estén afectando el funcionamiento del servidor, el cual lo verifica el especialista en mantenimiento de servicios generales.
	VERIFICACION DEL SOFTWARE	
	1	Encendemos el servidor
	2	Si observamos que el sistema operativo está fallando, se realiza un Backup del servidor.
	3	Una vez realizado el Backup procedemos a la reinstalación del sistema operativo y configuración como servidor.
	4	Se instala las aplicaciones
	5	Se restaura el Backup realizado.
	6	Configura los permisos de accesos a usuarios
	7	Se realiza pruebas de conectividad.
	8	Finaliza la reinstalación.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

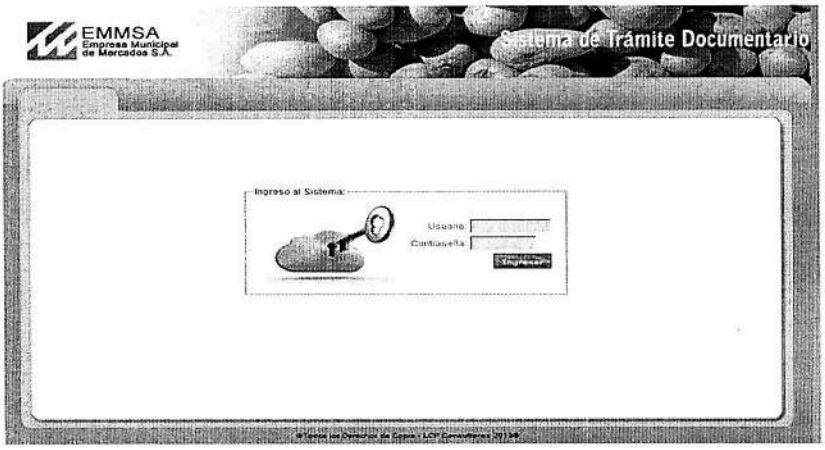
	RESTAURACION DEL EQUIPO	
	1	Identifica el Backup.
	2	Se empieza la restauración de la data o archivo
	3	Se verifica si la data o archivo restaurado en el servidor está completa.
	4	Se finaliza la restauración.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

Anexo: Plan de Recuperación
Falla de aplicativos propios de EMMSA

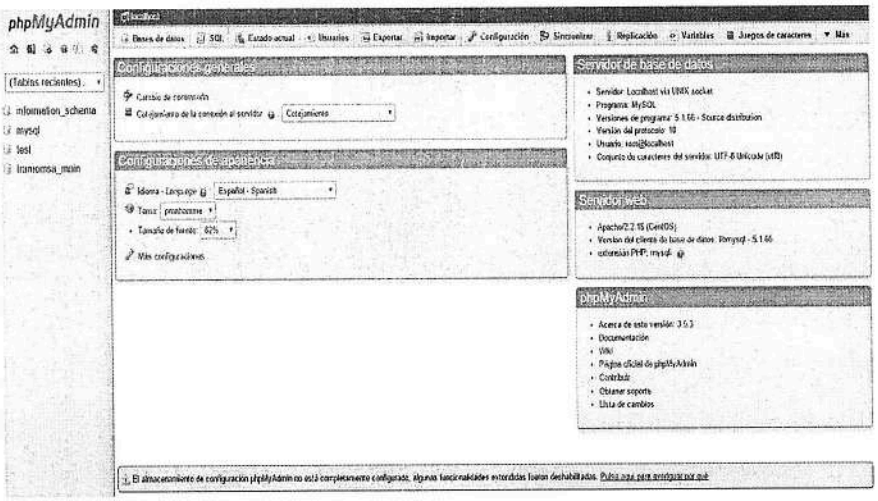
Sistema de Trámite Documentario

Existe un proceso de generación de Backup de la Base de datos el cual se realiza diariamente. Se envía una copia de la base de datos semanalmente en cinta de Backup a la empresa RANSA. De ser necesario con este Backup se puede restablecer el Sistema.	
Sistema Operativo	Linux Centos 6
Base de Datos	MySQL
Código Fuente	Php
usuario	Administrador Password: 123456
Dirección IP	10.60.0.6



1. Ingresamos a la dirección http://10.60.0.6/privado/phpMyAdmin/
2. Usuario: root, contraseña:123456

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA



Seleccionamos el esquema tramemsa_main

3. Seleccionamos la pestaña Exportar.
4. Seleccionamos Rápido.
5. Seleccionamos formato SQL.
6. Continuar y genera el SQL.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

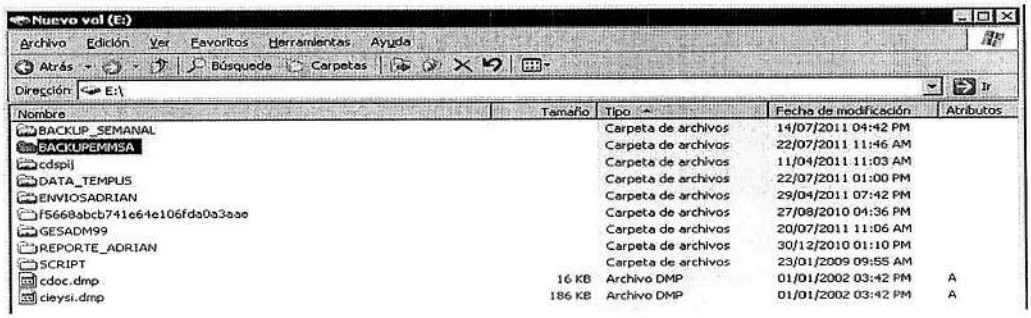
Anexo: Plan de Recuperación
Falla de aplicativos propios de EMMSA

Servidor de Archivos

Existe un proceso de generación de Backup de la Base de datos el cual se realiza semanalmente. Se envía una copia de la base de datos semanalmente en cinta de Backup a la empresa RANSA. De ser necesario con este Backup se puede restablecer el Sistema.	
Sistema Operativo	Windows Server 2003
usuario	Administrador Password: atenas
Dirección IP	10.60.0.4

PROCEDIMIENTO DE RESPALDO DE INFORMACIÓN EN EL SERVIDOR DE ARCHIVOS

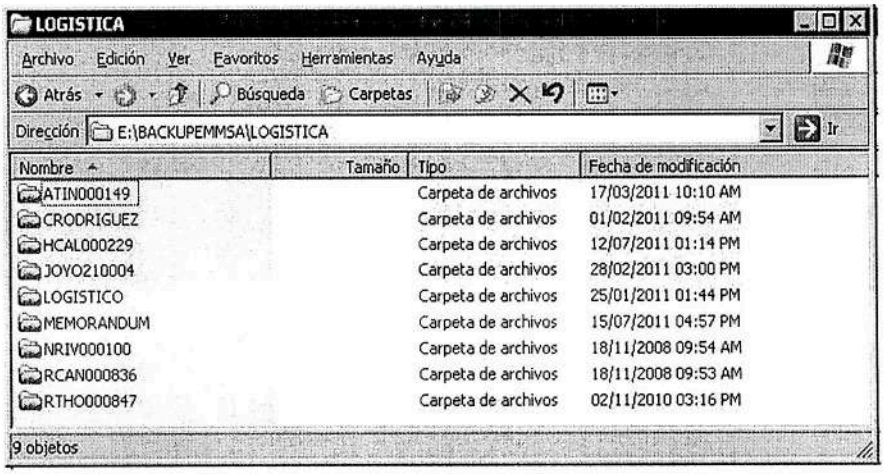
1. Nos ubicamos a la ruta de almacenamiento de datos.



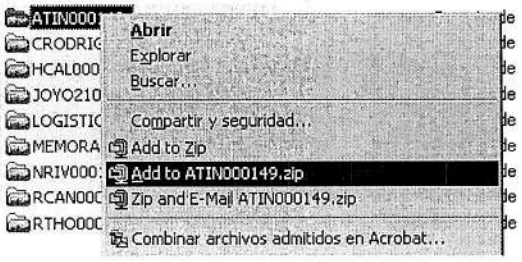
2. En BACKUPEMMSA se encontraran las carpetas con nombre de todas las áreas de la Empresa.

3. Entramos en cualquiera de las carpetas, por ejemplo entraremos a LOGISTICA.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA



4. Seleccionamos y damos click derecho a la carpeta ATIN000149, seguido le seleccionamos **Addto ATIN000149.zip.**



5. Se terminó el Zipeado de la carpeta de almacenamiento de archivos del usuario.

6. Ahora pasaremos al grabado en medio almacenamiento externo (DVD).

7. Seleccionamos el software para el proceso de grabado, en este caso usaremos el ROXIO.

8. Introducimos el DVD en la Lectora del Servidor de Archivos.

9. En el software seleccionamos **Datos-Disco de Datos-Agregar datos,** seguido le damos click en el botón rojo **.**En agregar datos agregamos los ZIP realizados anteriormente.

10. Se culminara el grabado en el dispositivo de almacenamiento externo.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Anexo: Plan de Recuperación
Falla en las Base de Datos Oracle, SQL de los servidores

Existe un proceso de generación de Backup de la Base de datos el cual se realiza semanalmente. Se envía una copia de la base de datos semanalmente en cinta de Backup a la empresa RANSA. De ser necesario con este Backup se puede restablecer el Sistema.	
Sistema Operativo	Windows Server 2003
usuario	Administrador Password: Emmsa@gmml
Dirección IP	10.70.0.40

BACKUP FÍSICO DE LA BASE DE DATOS

Los **backups físicos** son aquellos que copian físicamente los ficheros de la BD. Existen dos opciones: en **frío** y en **caliente**. Se dice que el Backup es en **frio** cuando los ficheros se copian cuando la BD está detenida. En **caliente** es cuando se copian los ficheros con la BD abierta y ejecutándose.

a. Del Backup en Caliente

Para este tipo de Backup, se ejecuta el archivo BACKUP.bat, el cual está asociado a una tarea programada llamada Backup. Esta tarea se ejecutará todos los días a las 8:00 am.

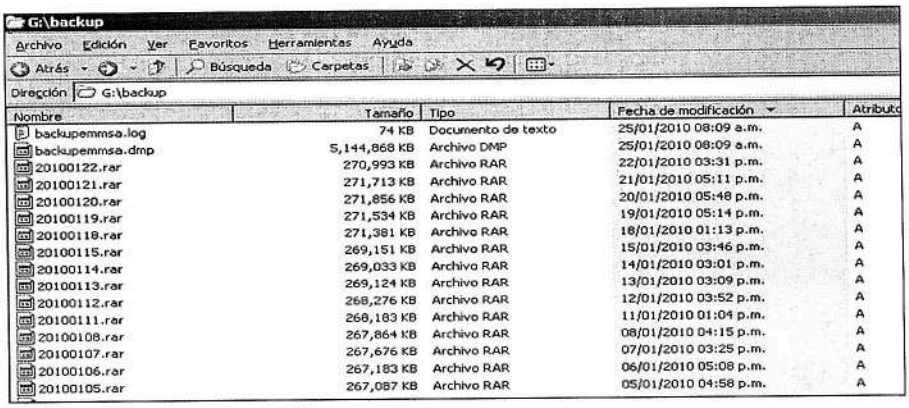
El script contenido en el archivo BACKUP.bat, es el siguiente:

Figura. Tarea Programada creada por el utilitario de Windows 2003 Server S

```
expsystem/sesamo@oraemmsa  buffer=61440   file=g:\backup\backupemmsa.dmp
owner=cpromero,jsarmiento,jroca,planil,cobranzas
log=g:\backup\backupemmsa.log COPIA.EXE
```

Posteriormente, se empaqueta y comprime los archivos: **backupemmsa.dmp** y **backupemmsa.log.** A continuación se muestra información de los backups.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA



Nombre	Tamaño	Tipo	Fecha de modificación	Atributo
backupemmsa.log	74 KB	Documento de texto	25/01/2010 08:09 a.m.	A
backupemmsa.dmp	5,144,868 KB	Archivo DMP	25/01/2010 08:09 a.m.	A
20100122.rar	270,993 KB	Archivo RAR	22/01/2010 03:31 p.m.	A
20100121.rar	271,713 KB	Archivo RAR	21/01/2010 05:11 p.m.	A
20100120.rar	271,856 KB	Archivo RAR	20/01/2010 05:48 p.m.	A
20100119.rar	271,534 KB	Archivo RAR	19/01/2010 05:14 p.m.	A
20100118.rar	271,381 KB	Archivo RAR	18/01/2010 01:13 p.m.	A
20100115.rar	269,151 KB	Archivo RAR	15/01/2010 03:46 p.m.	A
20100114.rar	269,033 KB	Archivo RAR	14/01/2010 03:01 p.m.	A
20100113.rar	269,124 KB	Archivo RAR	13/01/2010 03:09 p.m.	A
20100112.rar	268,276 KB	Archivo RAR	12/01/2010 03:52 p.m.	A
20100111.rar	268,183 KB	Archivo RAR	11/01/2010 01:04 p.m.	A
20100108.rar	267,864 KB	Archivo RAR	08/01/2010 04:15 p.m.	A
20100107.rar	267,676 KB	Archivo RAR	07/01/2010 03:25 p.m.	A
20100106.rar	267,183 KB	Archivo RAR	06/01/2010 05:08 p.m.	A
20100105.rar	267,087 KB	Archivo RAR	05/01/2010 04:58 p.m.	A

Del Backup en Frío

Antes de realizar el backup en frío, se deberá detener los siguientes servicios:

→Oracle

OracleMTSRecovery Service

OracleOrahome92Agent

OracleOrahome92HTTP

OracleOrahomeTnslistener Service

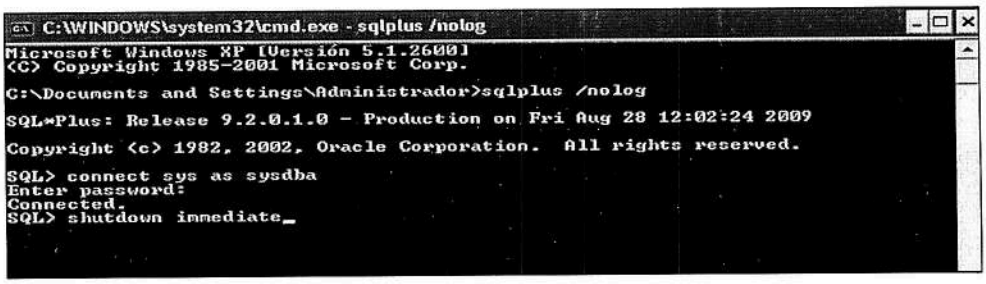
OracleOraHomeORAEMMSAService

Luego, se deberá abrir el cmd y ejecutar los siguientes comandos:

C:\sqlplus /nolog

SQL>connect sys as sysdba

SQL> shutdownimmediate



Copiar las siguientes carpetas:

UNIDAD F: →oracle

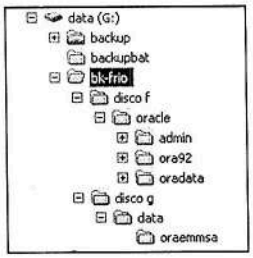
→admin

→ora92

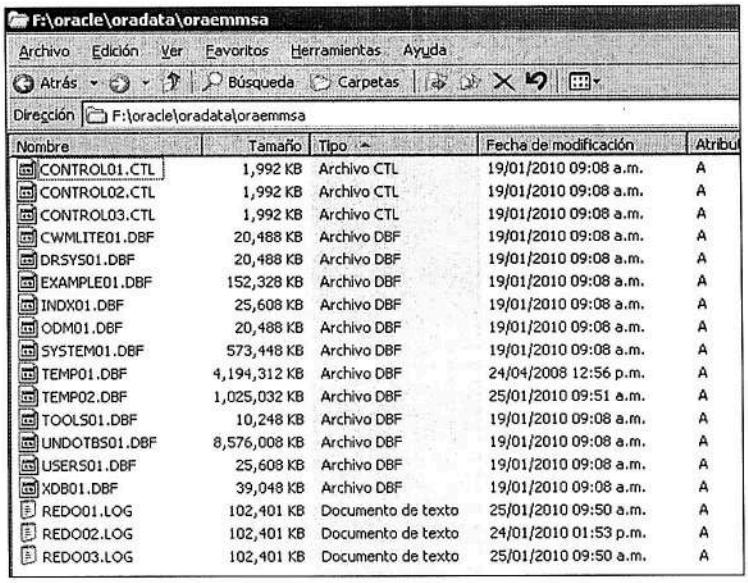
→oradata

UNIDAD G: →data

→oraemmsa



SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA



Nombre	Tamaño	Tipo	Fecha de modificación	Atribu
CONTROL01.CTL	1,992 KB	Archivo CTL	19/01/2010 09:08 a.m.	A
CONTROL02.CTL	1,992 KB	Archivo CTL	19/01/2010 09:08 a.m.	A
CONTROL03.CTL	1,992 KB	Archivo CTL	19/01/2010 09:08 a.m.	A
CWMLITE01.DBF	20,488 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
DRSYS01.DBF	20,488 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
EXAMPLE01.DBF	152,328 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
INDX01.DBF	25,608 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
ODM01.DBF	20,488 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
SYSTEM01.DBF	573,448 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
TEMP01.DBF	4,194,312 KB	Archivo DBF	24/04/2008 12:56 p.m.	A
TEMP02.DBF	1,025,032 KB	Archivo DBF	25/01/2010 09:51 a.m.	A
TOOLS01.DBF	10,248 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
UNDOTBS01.DBF	8,576,008 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
USERS01.DBF	25,608 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
XDB01.DBF	39,048 KB	Archivo DBF	19/01/2010 09:08 a.m.	A
REDO01.LOG	102,401 KB	Documento de texto	25/01/2010 09:50 a.m.	A
REDO02.LOG	102,401 KB	Documento de texto	24/01/2010 01:53 p.m.	A
REDO03.LOG	102,401 KB	Documento de texto	25/01/2010 09:50 a.m.	A

Figura. *Se observa los archivos contenidos dentro de la carpeta oraemmsa.*

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

RECUPERACION DE BASE DE DATOS POR IMPORTACION DE DATA (USANDO EL .DMP BACKUP EN CALIENTE)

Ejecutar los siguientes comandos y sentencias para la creación de usuarios y esquemas de la base de datos.

```
SQL> CREATE USER CPROMERO
  2  IDENTIFIED BY **********
  3  DEFAULT TABLESPACE USERS
  4  TEMPORARY TABLESPACE TEMP
  5  QUOTA UNLIMITED ON USERS;
User created.

SQL> GRANT CONNECT TO CPROMERO;
Grantsucceeded.

C:\ imp system/******* fromuser=CPROMERO touser=CPROMERO commit=y
ignore=y file=backupemmsa.dmp log=backupemmsa.log
       Usuario/Esquema: CPROMERO
```

```
C:\DBEMMSA RECUPERACION>imp system/al2jl2r2 fromuser=CPROMERO touser=CPROMERO co
mmit=y ignore=y file=backupemmsa.dmp log=backupemmsa.log

Import: Release 9.2.0.1.0 - Production on Thu Feb 25 12:33:42 2010

Copyright (c) 1982, 2002, Oracle Corporation.  All rights reserved.


Connected to: Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.1.0 - Production
```

```
SQL> GRANT CONNECT TO CPROMERO;

Grant succeeded.

SQL>
```

```
Connected to:
Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.1.0 - Production

SQL> CREATE USER CPROMERO
  2  IDENTIFIED BY CPR6022
  3  DEFAULT TABLESPACE USERS
  4  TEMPORARY TABLESPACE TEMP
  5  QUOTA UNLIMITED ON USERS;

User created.

SQL>
```

Usuario/Esquema : PLANIL

Usuario/Esquema : JROCA

Usuario/Esquema : JSARMIENTO

Usuario/Esquema : COBRANZAS

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

RECUPERACION DE LA BASE DE DATOS USANDO LOS DATAFILE (BACKUP EN FRIO)

El segundo método para la recuperación de la base de datos, es mediante los archivos generados por un backup en frio. A continuación se detalla el procedimiento para realizar el backup en frio:

Procedimiento para realizar el backup en frio en ORAEMMSA.

(ORAEMMSA) Ubicar los archivos necesarios para la recuperación de la base de datos; para esto se puede ejecutar la vista V$DATAFILE, el cual nos mostrará la ubicación de estos archivos.

```
C:\Documents and Settings\Administrador>sqlplus "sys as sysdba"
SQL*Plus: Release 9.2.0.1.0 - Production on Jue Mar 18 09:06:38 2010
Copyright (c) 1982, 2002, Oracle Corporation.  All rights reserved.
Enter password:

SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
```

```
SQL>SELECT name FROM V$datafile;

F:\ORACLE\ORADATA\ORAEMMSA\SYSTEM01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\UNDOTBS01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\CWMLITE01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\DRSYS01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\EXAMPLE01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\INDX01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\ODM01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\TOOLS01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\USERS01.DBF
F:\ORACLE\ORADATA\ORAEMMSA\XDB01.DBF
G:\DATA\ORAEMMSA\DDADMIN01.ORA
G:\DATA\ORAEMMSA\IDSISTEM01.ORA
G:\DATA\ORAEMMSA\IESISTEM01.ORA
G:\DATA\ORAEMMSA\IDSISTEM02.ORA
G:\DATA\ORAEMMSA\IDSISTEMA03.ORA
G:\DATA\ORAEMMSA\IDSISTEM03.ORA
```

En la base de datos; abrir el símbolo del sistema (Inicio → Ejecutar →cmd), y conectarse como sysdba, luego ejecutar el comando shutdownimmediate.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

(ORAEMMSA) Copia de los archivos (Datafiles) a un lugar seguro; ubicar y copiar las carpetas contenedoras de los datafiles y copiarlos a una unidad externa o a otra unidad del disco.

(ORAEMMSA) Levantar la base de datos; abrir el símbolo del sistema (Inicio → Ejecutar →cmd), y conectarse como sysdba, luego ejecutar el comando startup.

```
SQL> startup
ORACLE instance started.
Total System Global Area  135338868 bytes
Fixed Size                   453492 bytes
Variable Size             109051904 bytes
Database Buffers           25165824 bytes
Redo Buffers                 667648 bytes
Database mounted.
```

```
Enter user-name: sys as sysdba
Enter password:
Connected to:
Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.1.0 - Production
SQL> ALTER DATABASE BACKUP CONTROLFILE TO TRACE RESETLOGS;
Databasealtered.
```

(ORAEMMSA) Generar script para clonar la base de datos en un servidor de respaldo; abrir el símbolo del sistema (Inicio → Ejecutar →cmd), y conectarse como sysdba, luego ejecutar el comando alter databasebackupcontrolfileto trace resetlogs. Esto generará un archivo .trc, ubicado en la carpeta udump, para saber donde se encuentra este archivo, verificar el valor del parámetro (user_dump_dest). Para nuestro caso ubicar el último trace file generado en la ruta: **F:\oracle\admin\oraemmsa\udump.**

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

(ORAEMMSA) Ubicar el archivo .trc, generado anteriormente y renombrarlo con el nombre **crearoraemmsa.sql**, y copiarlo al equipo **RESPALDO** (siendo este equipo, donde se restaurará la base de datos).

(ORAEMMSA) Ubicar los datafiles copiados en el backup en frio y copiarlo al equipo **RESPALDO** (siendo este equipo, donde se restaurará la base de datos)

Procedimiento para clonar la base de datos o recuperarla en otro servidor (RESPALDO).

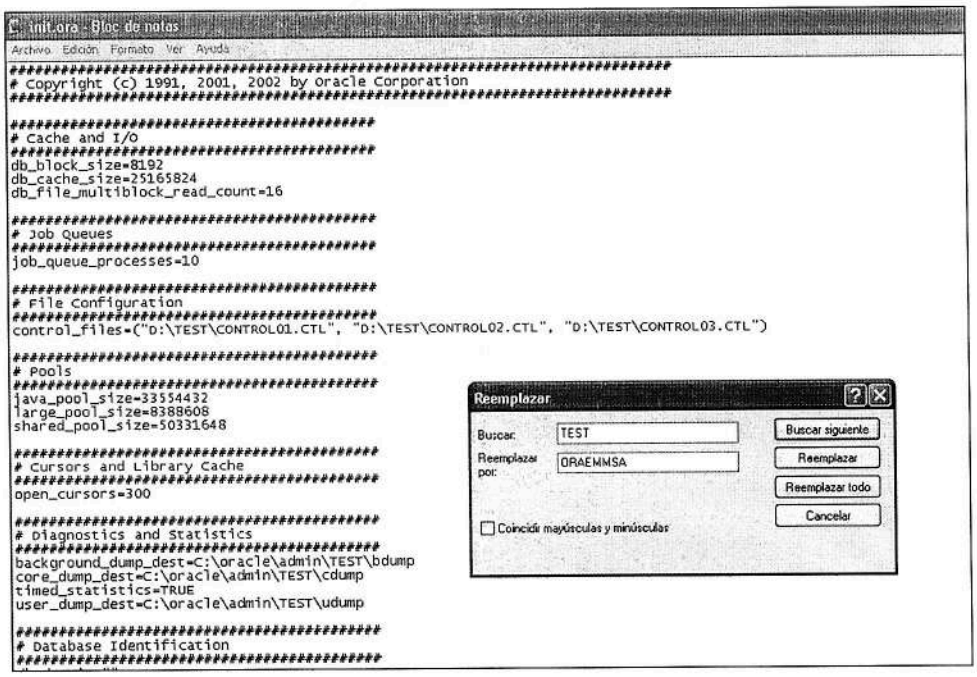
(RESPALDO) generar un árbol de carpetas donde se ubicaran los datafiles copiados del servidor ORAEMMSA. Para nuestro caso en la ruta **'C:\oracle\admin\'** crearemos la siguiente estructura de carpetas.

```
C:\oracle\admin\
                    -oraemmsa
                            -udump
                            -bdump
                            -cdump
                            -create
                            -pfile
-init.ora (archivo copiado de ORAEMMSA)
```

(ORAEMMSA) Copiar el archivo **init.ora**, ubicado en la carpeta pfile de la base de datos ORAEMMSA, y pegarlo en la carpeta pfile del servidor **RESPALDO.**

(RESPALDO) Abrir y editar el archivo **init.ora,** usualmente se reemplaza la ruta donde se ubican los datafiles copiados anteriormente.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

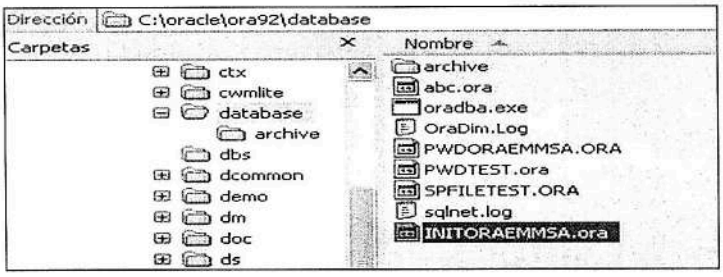


(RESPALDO) Abrir y editar el archivo **crearoraemmsa.sql,** reemplazando las rutas correctas donde se encuentren los datafiles y borrando los comentarios, de tal manera que al final obtengamos algo como el siguiente script:

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

```
STARTUP NOMOUNT
CREATE CONTROLFILE REUSE DATABASE "ORAEMMSA" RESETLOGS  NOARCHIVELOG
    MAXLOGFILES 50
    MAXLOGMEMBERS 5
    MAXDATAFILES 100
    MAXINSTANCES 1
    MAXLOGHISTORY 453
LOGFILE
  GROUP 1 'C:\ORACLE\ORADATA\ORAEMMSA\REDO01.LOG'  SIZE 100M,
  GROUP 2 'C:\ORACLE\ORADATA\ORAEMMSA\REDO02.LOG'  SIZE 100M,
  GROUP 3 'C:\ORACLE\ORADATA\ORAEMMSA\REDO03.LOG'  SIZE 100M
DATAFILE
  'C:\ORACLE\ORADATA\ORAEMMSA\SYSTEM01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\UNDOTBS01.DBF',
'C:\ORACLE\ORADATA\ORAEMMSA\CWMLITE01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\DRSYS01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\EXAMPLE01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\INDX01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\ODM01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\TOOLS01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\USERS01.DBF',
  'C:\ORACLE\ORADATA\ORAEMMSA\XDB01.DBF',
'G:\DATA\ORAEMMSA\DDADMIN01.ORA',
  'G:\DATA\ORAEMMSA\IDSISTEM01.ORA',
  'G:\DATA\ORAEMMSA\IDSISTEM02.ORA',
  'G:\DATA\ORAEMMSA\IDSISTEM03.ORA',
  'F:\DATA\ORAEMMSA\IESISTEM01.ORA',
  'F:\DATA\ORAEMMSA\IDSISTEMA03.ORA'
CHARACTER SET US7ASCII;
```

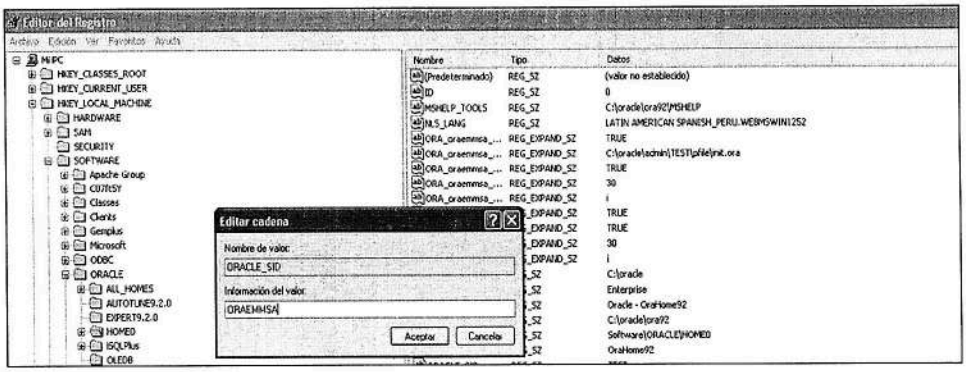
(RESPALDO) Copiar el archivo **init.ora,** en la ruta 'C:\ORACLE\ORA92\DATABASE\' y renombrarlo como **initoraemmsa.ora**, donde oraemmsa es el nombre de la base de datos a crear.




```
C:\>oradim -new -sidoraemmsa -intpwdoraemmsa -startmode auto -pfile
C:\oracle\
admin\TEST\pfile\init.ora
```

(RESPALDO) Crear el servicio oraemmsa, desde el cmd. Ejecutar el siguiente comando:

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA



(RESPALDO) Cambiar el ORACLE_SID, en el servidor, desde el cmd, se puede ejecutar el comando: SET ORACLE_SID=ORAEMMSA, o desde el REGEDIT, cambiar dicho parámetro.

(RESPALDO) Ejecutar el script **crearoraemmsa.sql,** en el cmd ubicarse en el directorio donde se encuentra el script y logearse como sysdba. Luego ejecutar con el @crearoraemmsa.

```
Enter user-name: sys as sysdba
Enter password:
Connected to an idle instance.
SQL> @crearoraemmsa;
ORACLE instance started.
Total System Global Area  135338868 bytes
Fixed Size                   453492 bytes
Variable Size             109051904 bytes
Database Buffers           25165824 bytes
Redo Buffers                 667648 bytes

Control file created.
```

C

utar el alter databaseopenresetlogs;

```
SQL>alter database open resetlogs;
```

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

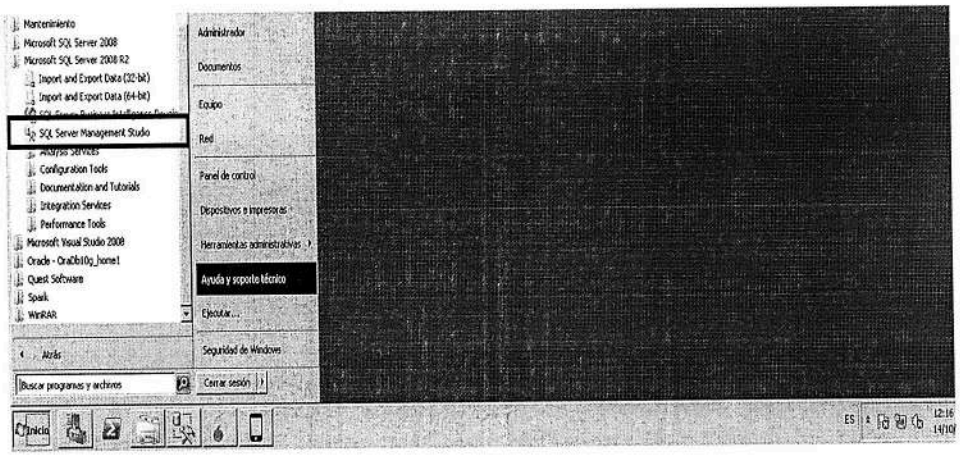
Anexo: Plan de Recuperación
Servicio Telefónico.

En caso de corte contactarse con **CLARO** para ver el estado de la red RDSI si esta se encuentra operativa, en caso de fallas ponerse en contacto con el proveedor para la revisión de la central telefónica. Se cuenta con 75 anexos y una central telefónica de recepción de llamadas.	
Central Telefónica Samsung	
Modelo	Office Serv 7200
Serie	S2JC407547J
Contactos	Central Telefonica MR TECNYSOL S.R.L. INES GUARDIA SOLA ventas@ mrtecnysol.com Teléfono:2269381 Celular:990396044 CLARO AMERICA MOVIL PERU S.A.C. DAVID ALEXIS GIOVE RAMOS david.giove@claro.com.pe Teléfono: 6131000 Celular: 982151696
Software tarificador	IP: 10.60.0.5 usuario: Administrador contraseña: ADM01$

15.1. Plan de Respaldo:

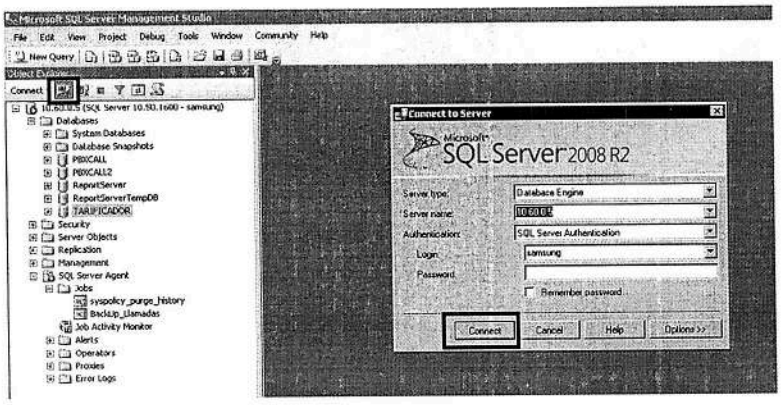
- Se realiza Back-Up diario de las llamadas realizadas de cada anexo, se realiza el siguiente procedimiento:
  - **a.** Inicio
  - **b.** Todos los programas
  - **c.** Microsoft SQL Server 2008 R2
  - **d.** SQL Server Managment Studio.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA



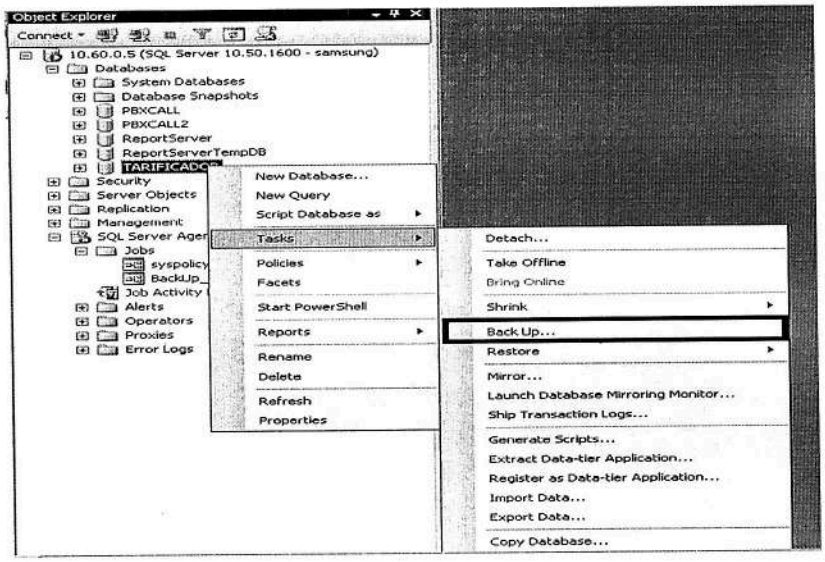
e. Clic en la imagen de conectar como indica en la imagen.

f. Presionar el botón Connect.

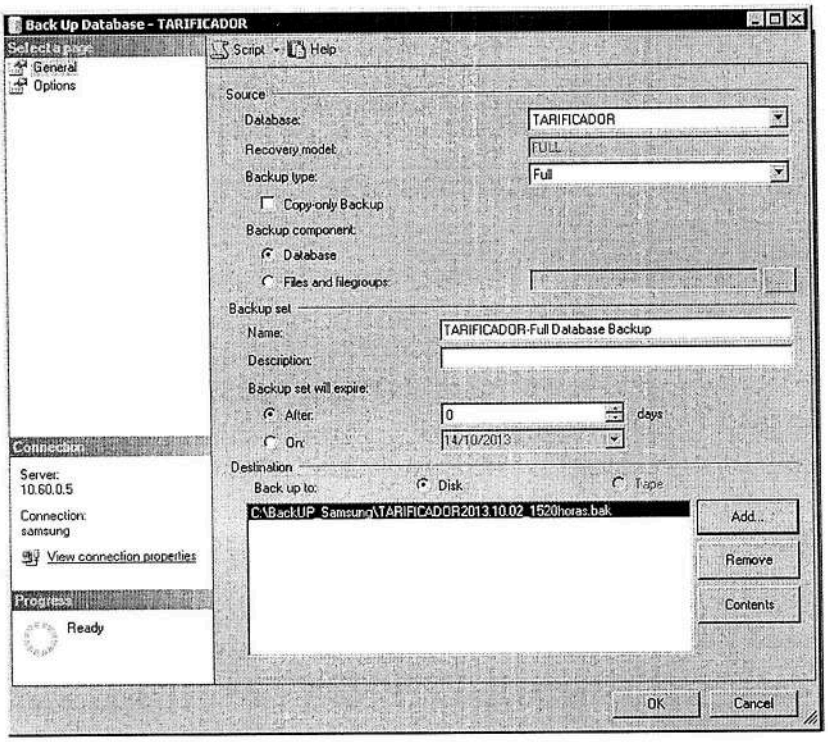


g. Clic derecho en TARIFICADOR
h. Task – Back Up

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA



i. Clic en "Add"
j. Escoger la ruta donde se va a grabar el Back – Up
k. OK
l. OK
m. Backup generado.



SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Anexo: Plan de Recuperación

Servicio de Video Vigilancia CCTV

El Sistema integral de video vigilancia está conformado por una plataforma basada en conectividad IP, el cual integra cámaras DOMO PTZ, cámaras fijas, backbone de fibra óptica para interconexión de las cámaras con el centro de control, cableado estructurado para datos, estación de monitoreo y control, matriz virtual para visualización y despliegue de las cámaras, sistemas de grabación NVR con arreglos de discos RAID 5 para su almacenamiento (Si falla un disco se repone automáticamente sin perder datos hasta reponer el disco dañado) además ante una caída eléctrica se cuenta con un sistema de protección antes cortes de energía eléctrica (UPS). Problemas de configuración contactar con el proveedor de mantenimiento CCTV.	
Software	ViconNet NVR 5.6, AVIGILON 5, Luxriot 2.2, ViconNet Virtual 6.6, ViconNet Núcleo 7.1
Contactos	Hermogenes Untiveros Gerente General de UBATEC SA Cel. 996544455 Email. h untiveros@ubatec.net
Cantidad Cámaras Domos	17
Cantidad Cámaras Fijas	39
Servidores NVR	10.30.0.28 – 10.30.0.29
Servidor Núcleo	10.30.0.20
Matriz de Video	10.30.0.21

Proceso de Respaldo y Restauración del Sistema CCTV

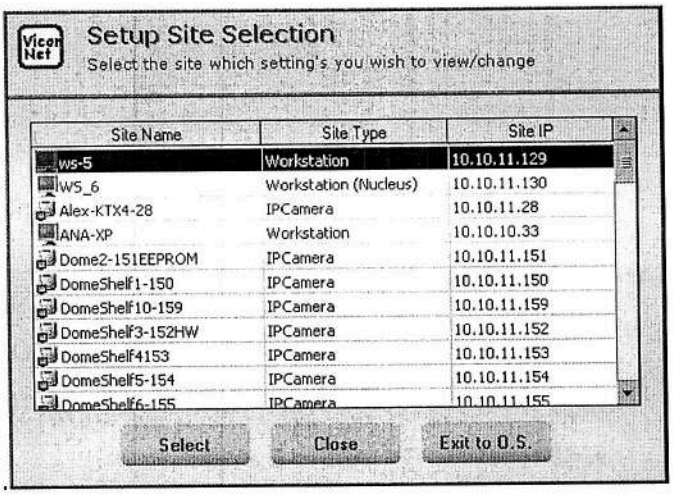
El sistema ViconNet automáticamente respalda todos los ajustes del sistema cada vez que usted corre la aplicación del ViconNet.

Además, también se puede respaldar manualmente los ajustes del sistema en cualquier momento, a cualquier locación de red, o restaurar los ajustes a aquellos que fueron guardados previamente.

Para respaldar manualmente o restaurar ajustes del sistema:

1. Desde la ventana principal del ViconNet, oprima Setup. La ventana Selección de Sitio de Ajustes desplegada, como se muestra en la siguiente imagen

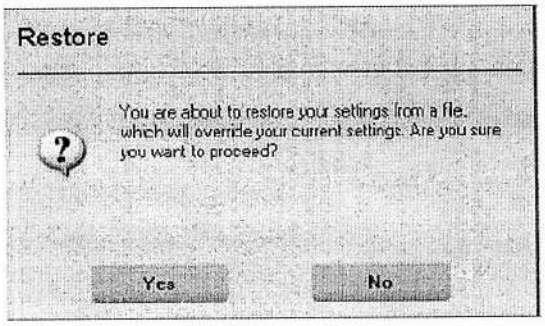
SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA



2. En esta ventana deberá seleccionar el equipo que desea hacer un respaldo o restaurar. Luego deberá oprimir Select.

3. Para respaldar los ajustes, oprima Backup . Una ventana de buscador de archivo es desplegada. Seleccione la dirección de respaldo requerida y oprima **OK**. Es altamente recomendado que usted respalde los ajustes a un disco o CD, en caso que el disco duro falle. Después que usted ha grabado los ajustes al disco o CD, etiquételo con el nombre del archivo y la fecha en la cual fue creado.

4. Para restaurar los ajustes, oprima Restore . Y aparecerá una nueva ventana como la siguiente imagen.



SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

5. Para continuar, haga clic en **YES**. Aparecerá una ventana del explorador de archivos. Navegue hasta el archivo de copia de seguridad que desea restaurar y haga clic en **OK**.

   NOTA: Recuerde que la locación de respaldo para propósitos de restauración. Es importante restaurar los ajustes del sistema en el mismo equipo en el cual el respaldo fue ejecutado.

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUB-GERENTE
EMMSA

EMMSA
Empresa Municipal de Mercados S.A.

Anexo: Plan de Recuperación
Interrupción del Fluido Eléctrico

Entra automáticamente en funcionamiento los 2 UPS : 1 UPS de 10Kva (Servidores) y 1 UPS de 8Kva (CCTV) Esto mientras se pone en marcha el grupo electrógeno del GMML el cual es realizado por el personal electricista del GMML.	
Jefe de Electricistas	Daniel Candiotti Bravo
Teléfono	996273660
Especialista en Mantenimiento de Equipos	Adrián Alvarado Blácido
Teléfono	999268188

DESCRIPCION DEL PROCEDIMIENTO		
PROCEDIMIENTO: CORTE DEL FLUIDO ELECTRICO		
AREA: SUBGERENCIA DE INFORMATICA		
RESPONSABLE	**ACT. NUMERO**	**DESCRIPCION DE ACTIVIDADES**
DEPARTAMENTO DE INFORMATICA	**APAGADO AUTOMATICO DE LOS SERVIDORES UPS**	
	1	Se verifica si el UPS está configurado para el apagado automático de los servidores.
	2	Entonces cuando no haya fluido eléctrico los servidores se apagaran automáticamente.
	APAGADO MANUAL DE LOS UPS	
	1	Si el UPS no está programado para el apagado automático, se recurre al apagado manual de los servidores.
	2	Nos dirigimos a Inicio – Apagar – Apagar.
	3	Una vez apagado el servidor, se apaga el UPS.
	4	Cuando se restablece el fluido eléctrico se enciende el UPS y los servidores.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

	5	Se verifica el correcto funcionamiento de los servidores y UPS.

EMMSA
Empresa Municipal de Mercados S.A.

Anexo: Plan de Recuperación

Servicio de Internet

Se verifica que no exista un problema con el proveedor de Internet. (Telefónica) De no ser problema el proveedor, se revisa el firewall Fortigate 80c de persistir la falla se Restaura con un Backup la configuración.	
Router	
Modelo	Cisco 1900 Series
Código a brindar para gestiones Telefónica del Perú	CD: 94656
Velocidad Contratada	10 MB
Contacto Telefónica	Mario Segura Supervisión Servicios Internacionales y Centro de Gestión Mario.segura@telefonica.com RPM: #346086 Fijo: 2109714 William Tumbalobos Vásquez Jefe Gestión de Clientes y Servicios William.tumbalobos@telefonica.com Cel.: 996376491 RPM: #582318 Fijo: 2109611 Carmela Galarza Guillen Gerente de Gestión Integrada de clientes y Servicios Carmela.galarza@telefonica.com Cel.: 998707874 RPM: #582295 Fijo: 2109601
Rango IPs Públicos	181.65.178.24 - 181.65.178.31 200.48.72.112 – 200.48.72.112
Otros	Visualizar el tráfico del internet: http://www.cgrc.telefonica.com.pe Usuario: emmsa emumersa Password: 3mm5@ 3mum3rs4
Para averías en el servicio de internet llamar al número 1386 o 080016600 (opción 2, 2 ,1) Indicar que tenemos 3 circuitos digitales: CD 91805, CD 91807, **CD 94656 (Este es el de internet).** Indicar el ruc de la empresa: 20100164958 Y solicitar el número de ticket.	
Firewall	
Modelo:	FortiGate 80C
Serial Number:	FGT80C3911621343

SUB-GERENCIA DE INFORMÁTICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Partner:	EBD PERU S.A. Call Center: +(511) 712-5040
Contacto	Diana Pérez Asesor de Telecomunicaciones T.+ (511) 7125000 anexo 5017
Número de Contrato:	336259483867
Numero IP Wan-Lan	181.65.178.26 – 10.60.0.254
Acceso	https://10.60.0.254 usuario : admin password: l3t@cl@1++

SUB-GERENCIA DE INFORMATICA
V°B°
I. RAMIREZ
SUBGERENTE
EMMSA

Anexo: Plan de Prevención

Lista Teléfonos de Emergencia

LISTA TELÉFONOS DE EMERGENCIA	
BOMBEROS	
Central de Emergencia	**116**
Cía. Bomberos	**478-1099**
EMERGENCIAS POLICIALES	
Escuadro de Emergencia	371-6319
Comisaría de Santa Anita	478-2232
Águilas Negras	362-3277

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

Anexo: Plan de Recuperación

Dominio: EMMSA.COM.PE

Registro	:	1 de Diciembre, 2003
Vence	:	30 de Noviembre, 2018
Estado	:	Activo
Contacto	:	Edwin Jiménez – 5182800

DNS

- dns1.unired.net.pe
- dns2.unired.net.pe
- ns.rcp.net.pe
- ns2.rcp.net.pe

Registros MX/CNAME/A/TXT

Nombre	Tipo	Contenido	Pri.
emmsa.com.pe	SOA	NS.RCP.NET.PE operador.rcp.pe 2014020600 7200 300 604800 7200	0
emmsa.com.pe	TXT	google-site-verification=VYaeI57p3rJql2j1W40L4Tl8vp9pyQmfJG8y1zewXkQ	0
emmsa.com.pe	MX	ASPMX.L.GOOGLE.COM	1
emmsa.com.pe	MX	ALT1.ASPMX.L.GOOGLE.COM	2
emmsa.com.pe	MX	ALT2.ASPMX.L.GOOGLE.COM	3
emmsa.com.pe	MX	ASPMX2.GOOGLEMAIL.COM	4
emmsa.com.pe	MX	ASPMX3.GOOGLEMAIL.COM	5
emmsa.com.pe	MX	ASPMX4.GOOGLEMAIL.COM	6
emmsa.com.pe	MX	ASPMX5.GOOGLEMAIL.COM	7
mail.emmsa.com.pe	CNAME	ghs.googlehosted.com.	0
estadistica.emmsa.com.pe	A	181.65.178.29	0
www.emmsa.com.pe	A	181.65.178.30	0
ftp.emmsa.com.pe	A	181.65.178.30	0
camaras.emmsa.com.pe	A	181.65.178.30	0

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

CONTROL DIARIO DEL GRUPO ELECTRÓGENO

ANTES DE ARRANCAR

1. Verificar el nivel correcto del aceite.
2. Verificar el nivel de agua en el radiador.
3. Verificar la tensión de fajas del ventilador.
4. Avisar cuando el nivel de petróleo esté full, Verificar el nivel del agua en la batería.

EN FUNCIONAMIENTO

1. La temperatura no debe sobrepasar los 90°C.
2. La frecuencia debe mantenerse en 60Hz.
3. EL voltaje debe mantenerse en 220 ~ 400V.
4. El amperaje máximo aproximado será de 80A.

La presión del aceite: Si está por debajo de 30psi, apagar el grupo.

5. La aguja indicadora de carga de batería no debe estar en el lado negativo.
6. Observar si existe presencia de fuga de aceite en el motor, agua de radiador y acido en la batería.
7. Observara si hay humo en el escape, vibraciones excesivas o ruido extraño.

INSTRUCCIONES PARA OPERAR EL GRUPO ELECTRÓGENO

PARA ARRANCAR (MANUAL)

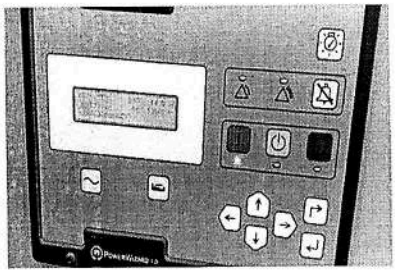
1. Verificar que la válvula de combustible este abierta.
2. Verificar que el selector este en off.
3. Verificar que el interruptor general del grupo esté en off (Palanca abajo).
4. Presionar por 15 segundos el botón **INGINE PREHEAT**.
5. Con una mano girar la llave del encendido a la posición RUN y con la otra presionar el botón **START BY PASS**.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

6. Cuando se siente el disparo de la válvula, continuar el giro de la llave a la posición **CRANK**; apenas encienda, dejar que la llave regrese a RUN mientras se va soltando poco a poco el botón **START**.
7. Ver el Display.
8. Dejar que caliente el motor unos 3 a 10 minutos aproximadamente y luego los parámetros de energía estén correctas.
9. Poner el interruptor general en **ON** (Palanca arriba)

PARA ARRANCAR (AUTOMÁTICO)

1. Ver el display y compara con el manual que todos los parámetros estén correctos.



PARA PARAR

1. Poner el interruptor general del grupo a la posición **OFF** (Palanca abajo).
2. Desacelerar al mínimo (Botón rojo).
3. Poner el selector en **OFF**, esperar 3 minutos.
4. Bajar la llave de encendido a **OFF**.

Anexo: Plan de Recuperación

CONTROL DIARIO DE CAMARAS DOMOS-PTZ Y FIJAS

RECOMENDACIONES

- Debe estar limpia y ordenada la Sala de Video Cámaras, muebles y útiles de escritorio.
- Verificar que los cabales que están conectados a las computadores y monitores tano de escritorio como los monitores de pared estén en buen estado
- Verificar el estado de los equipos de cómputo, Monitor PC, Teclados Mouse.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

- Realizar el proceso de estado de enlace de red LAN (área de red local), previa verificación de cable de red (plano).
- Verificar el estado de las imágenes de las cámaras DOMO –PTZ y FIJAS.
- A su relevo en cuaderno de cargo informar, cambios, modificaciones, recomendaciones y ocurrencias en su turno, preciso, y oportuno.
- Proceso de trabajo:
    - Verificar que las cámaras estén grabando constantemente y sin interrupciones.
    - Verificar que la calidad de imagen de la cámaras ya sea DOMO-PTZ o fijas que tengan nitidez y que este a colores cuando la cámara se está utilizando en video (Tiempo Real)
    - Monitor este en buen estado y que tenga nitidez
    - CPU que utiliza los operadores de cámaras deberá estar constantemente encendido y en buen estado.
    - No colocar USB o cables USB u otros dispositivos en los CPUs de los operadores de Cámaras.

TRABAJO EN PROGRESO PARA VIZUALIZAR LAS GRABACIONES (SISTEMA AVIGILON)

- Hacer Click en la pestaña que dice GRABCION.
- Seleccionar la cámara que se desea descargar el video
- Hacer Click en la ventana que está ubicado en la esquina inferior izquierda donde a continuación se pondrá la hora y la fecha.
- Hacer Click en el icono de PLAY y se podrá realizar la visualización de la grabación que se desea.

TRABAJO EN PROGRESO PARA DESCARGAR LAS GRABACIONES (SISTEMA AVIGILON)

- Hacer Click en la pestaña que dice GRABCION.
- Seleccionar la cámara que se desea descargar el video
- Hacer Click derecho en la cinta de grabación de color azul, a continuación aparecerá 2 opción en esas 2 opciones hacemos Click donde dice agregar marcador, luego aparecerá una ventana donde

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

ponemos la cámara que deseamos descargar la grabación y la fecha y la hora de la grabación que se requiera.

NOTA: Este procedimiento es igual con todas las cámaras que estén dentro del sistema AVIGILON.

RESTRICCIONES

- El ingreso de personas extrañas y no autorizadas.
- Manipulación de los equipos por personas extrañas.
- Instalar programas al sistema de cualquier tipo.
- Reproducir CD, DVD, mp3, mp4, celular, USB o discos de almacenamiento que no corresponde al sistema de CCTV.
- Consumir líquidos y alimentos junto al equipo de cómputo.
- Tratar de reparar, golpear, manipular los equipos y/o usar herramientas ajenas, copiar información y autorizar conexiones de cualquier sistema sin autorización.

ALCANCES

- Ocurrencias y fallas de equipos informar, al especialista de la, unidad mantenimiento de equipos y departamento de informática, por conducto regular, se atenderá las 24 horas en línea.
- Cambios y actualizaciones: el encargado de la Sala de Video Cámaras y el departamento de informática, alcanzará informes, comunicara y recomendara.
- El encargado de la Sala de Video Cámaras, realizara capacitación a los operadores de cámaras en caso que se cambie o se actualice las cámaras DOMO-PTZ y FIJAS del GMML.
- El encargado de la Sala De Video Cámaras, realiza control, supervisión, seguridad, y precisión – en los equipos y en las cámaras de CCTV de la sala de video cámaras.
- Cumplir el D.L-1218 emitida en el año 2015.
- Cumplir con el protocoló de sala de videocámaras.
- Cumplir con el reglamento establecido por EMMSA –GMML.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

TRABAJO EN PROGRESO PARA VISUALIZAR LAS GRABACIONES (SISTEMA VICON)

- Hacer Click derecho en la cámara que se desea ver la visualización de la grabación.
- Hacer Click en la fecha y la hora que se desea ver la visualización de la grabación
- Hacer Click en botón que dice OK para poder ver la visualización de la grabación

NOTA:

Este procedimiento es igual con todas las cámaras que estén dentro del sistema VICON.

TRABAJO EN PROGRESO PARA DESCARGAR LAS GRABACIONES (SISTEMA VICON

- Hacer Click derecho en la cámara que se desea ver la visualización de la grabación.
- Hacer Click en la fecha y la hora que se desea ver la visualización de la grabación.
- Hacer Click en botón que dice OK para poder ver la visualización de la grabación.

NOTA:

Este procedimiento es igual con todas las cámaras que estén dentro del sistema VICON.

SISTEMA AVIGILON

- Se ingresa con el usuario oper3
- Una vez que ingresamos seleccionamos la cámara que queremos ver
- Una vez que hagamos seleccionar la cámara que necesitamos hacemos Click en la opción que dice (GRABADO)

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

- Hacemos Click derecho en la línea de grabación que es de color azul donde aparecerá don opciones (Centrar Marcador, Agrega Marcador), hacemos Click en la opción que dice Agregar Marcador
- A continuación se abrirá una ventana para seleccionar la fecha y la hora que se requiere, después de re3alizar la selección se pone aceptar.
- Después de aceptar la selección aparecerá en la ventana de grabación una línea amarilla, la línea amarilla es la selección que se realizó con la fecha y hora.
- Donde aparece la linea amarilla hacemos click derecho y seleccionamos la opcion EXPORTAR
- Luego se hace Click donde dice INICIAR EXPORTACION
- Se va abrir una ventana donde te pide en donde se va guardar la descarga de la grabación.
- Seleccionamos la carpeta y luego hacer Click en guardar y comenzara a realizar la descarga.

SISTEMA VICON

- Se selección a la cámara que se requiere ver la grabación.
- Se hace Click derecho en la cámara seleccionada y se hace Click en la opción que dice (STAR PLAYBACK FROM TIME
- Se abrirá una mini ventana donde se puede seleccionar la fecha y la hora después de seleccionar se hace Click en la opción OK y se podrá visualizar la grabación de la cámara que se requiere.
- Se selecciona la cámara que se requiere descargar el video y se hace Click en la opción PLAYBACK
- Se abrirá una ventana donde se hará Click en el IP:10.30.0.29 y se abrirá una lista de cámaras.
- Se hará Click en la cámara que se requiere descargar la grabación y se cargara una línea de color azul (representa la grabación de la cámara seleccionada)
- Cuando cargue la grabación (Línea Azul) se seleccionara la fecha y la hora que se requiere
- La selección de fecha y hora del lado derecho es donde se va poner la hora y fecha inicial de las grabaciones y la selección de fecha y hora

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

de lado izquierdo es donde se va poner la hora y fecha final de las grabaciones la selección de fecha y hora lado izquierdo inferior en donde una línea de color guinda se posicionara en donde comenzara la grabación de la grabación.

- Después de haber realizado la selección de la fecha y hora se hará Click en la opción EXPORT VIDEO a continuación se abrirá una venta y donde dice FOLDER DESTINATION se s
- Seleccionara en que carpeta se va guardar la descarga del video, luego que se realizó la descarga se hace Click en la opción STAR.
- Después de hacer Click en la opción STAR se abrirá una ventana donde se realizara Click en CLOSE
- Y comenzara realizarse la descarga.

TRABAJO EN PROGRESO EN CASO QUE LAS SE QUEDEN SIN CONEXIÓN YA SEA SISTEMA AVIGILON O VICON.

- Después que el fluido eléctrico regrese a la sala de servidores se ingresa a la sala de servidores para encender los servidores ya sea AVIGILON o VICON donde cuando el servidor inicie sesión se ingresara al sistema ya sea AVIGILON o VICON para que las cámaras regresen.
- Cuando ya el sistema este operativo nuevamente, verificar si las cámaras que cuenta el GMML se puedan observar y monitorear en la Sala de Videocámaras.
- Caso que alguna cámara no cuente con conexión se procede al reinicio remoto desde el mismo servidor.
- En caso que se haya reiniciado la cámara desde el servidor, se coordina con Sub-Administración para que un electricista se dirija a la zona donde se encuentra la cámara desconectada y se percate si en esa aérea cuenta con luz.
- En caso que no cuente con luz el electricista buscara el problema si es dentro o fuera del GMML.
- En caso que el Electricista de turno comunique que el problema es por la zona donde se encuentra la cámara, tendremos que esperar hasta que el electricista habilite el fluido eléctrico por la zona donde se encuentra la cámara sin conexión.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA

- En caso que el electricista de turno indique que hay fluido eléctrico donde se encuentra la cámara sin conexión tendríamos que acércanos con el electricista de turno y verificar si en los gabinetes o en las llaves termo magnética de la cámara este en modo apagado (OFF) caso que este apagado se vuelve a poner en la posición de encendido (ON)
- En caso que la llave termo magnética este en modo encendido (ON) se coordinara con el área de Informática para que realice las coordinaciones del caso.

NOTA: Este procedimiento es igual con todas las cámaras que estén dentro del sistema AVIGILON O VICON solo cambiara el usuario y contraseña que cuenta y de los servidores ya que cada servido es independiente.

INTERVENCIÓN EXTERNA

1. En caso de presentarse un desperfecto donde se necesita desinstalar reparar o realizar actualizaciones para el CCTV se comunicara a la empresa externa de mantenimiento.

INTERVENCIÓN INTERNA

1. En caso de presenciar conflicto en el monitoreo del sistema CCTV.
2. En caso de presenciar desgaste del lente de las cámaras.
3. En caso de presenciar suciedad en las micas de las cámaras.
4. En caso de presenciar desconexión y no se pueda realizar vía remoto el reinicio de las cámaras.
5. En caso de Presenciar desperfectos de visualización en las cámaras y no se pueda solucionar vía remoto.

SUB-GERENCIA DE INFORMATICA V°B° I. RAMIREZ SUB-GERENTE EMMSA