

PLAN DE CONTINUIDAD TI

Contenido

INTRODUCCION 3

1. Objetivos y Alcance del Plan de Continuidad 4

1.1. Objetivo General 4

2. Alcance 4

3. Generalidades del Plan de Continuidad 4

4. Análisis del Entorno De La Empresa 5

5. Gestionar el plan 6

5.1. Normatividad asociada al Plan 6

6. Riesgos asociados a la continuidad del negocio 6

7. Roles y Responsabilidades 10

8. Desarrollo de las estrategias de Continuidad de TI 10

9. Plan de Capacitación, Comunicaciones y Sensibilización de Seguridad y Privacidad de la Información. 11

10. Evaluación de Impactos Operacionales 11

10.1. Identificación de Procesos Críticos 12

10.2. Establecimiento de Tiempos de Recuperación 12

10.3. Continuidad Del Servicio Conexión Internet 14

10.4. Soporte Siep 16

10.5. Soporte Hosting 16

10.6. Soporte Remoto 18

10.7. Backups 18

10.8. Restauración 19

11. Estrategia De Vuelta A La Normalidad 19

Conclusiones 20

INTRODUCCION

Con el fin de contar con una herramienta que nos permita prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo a los EMPRESA DE ACUEDUCTO Y ALCANTARILLADO SA E.S.P la Entidad consolidó una serie de acciones para iniciar el *Plan de continuidad del negocio* que, diseñadas y ejecutadas de forma planificada, permitirían responder de manera eficiente ante una eventualidad, restablecer en menor tiempo la prestación de los servicios y mitigar el impacto negativo de la pérdida de recursos.

El Plan de Continuidad de la entidad, será el mecanismo que le brindara la seguridad requerida para mantener los procesos claves de la entidad en óptimo funcionamiento ante una falla de muy alto impacto. Ante un evento crítico, este plan se activará y se podrá reaccionar en los tiempos adecuados para asegurar que los procesos claves sigan funcionando o se recuperen en el menor tiempo posible, mitigando de esta forma el impacto generado por dichos eventos negativos.

1. Objetivos y Alcance del Plan de Continuidad

1.1. Objetivo General

Definir las actividades preventivas, defectivas y correctivas para reaccionar de manera eficiente ante una eventualidad que comprometa el desarrollo de las actividades cotidianas, en la prestación del servicio.

- ✔ Objetivos específicos
- ✔ Asignar responsabilidades al personal designado
- ✔ Identificar las actividades críticas, los recursos y los procedimientos necesarios para llevar a cabo las operaciones durante las interrupciones prolongadas del servicio
- ✔ Asegurar una pronta recuperación en los servicios críticos para los Grupos de Valor
- ✔ Disminuir los tiempos de interrupción de la operación de los procesos
- ✔ Proteger los bienes de la empresa de Acueducto y Alcantarillado SA E.S.P de manera adecuada.

2. Alcance

El plan de continuidad inicia con la identificación y socialización de los elementos críticos en EISCUCUTA SA E.S.P que puedan definirse como incidente o desastre que impidan continuar la operación y finaliza con el análisis y acciones de mejora identificadas de la reacción ante la situación presentada mínimo una vez al año (simulacro o realidad)

3. Generalidades del Plan de Continuidad

El Plan de Continuidad reúne un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la misionalidad de la entidad y la prestación de sus servicios se establece en tres momentos:

- ✔ Preventivo: Se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan articular a la gestión institucional en los diferentes procesos.
- ✔ Reactivo: dirigido a fortalecer las políticas internas y comunicarlas oportunamente para ponerlas en marcha una vez detectada la contingencia.
- ✔ Recuperación: enfocado en las actividades a desarrollar en el momento de atender una contingencia.

4. Análisis del Entorno De La Empresa

Externo

- Factores Económicos: demoras o dificultades para el traslado de recursos.
- Factores Políticos: Cambio de jefes.
- Factores Sociales: Manifestaciones y protestas frecuentes en el centro de la ciudad, dificultad de acceso para el ciudadano y los servidores
- Factores Tecnológicos: Ataques externos a la información y las herramientas tecnológicas.
- Factor es Medio Ambientales: incendios, terremotos, Inundaciones, desastres naturales.

Internos:

- Financieros: cambios frecuentes en el plan adquisiciones, demoras en la apropiación de recursos.
- Personal: Planta de personal insuficiente, nuevas exigencias de competencias del personal en el nuevo modelo de operación, tiempo insuficiente para el desarrollo de habilidades, alta rotación de personal
- Tecnología: desconocimiento de un Plan estratégico de TI, fallas en la infraestructura tecnológica, fallas en el sistema de seguridad de la información, desconocimiento de los niveles de responsabilidad y autoridad frente a los

sistemas.

- Estratégicos: Fallas en la comunicación interna, solicitud de información múltiple, fallas en los sistemas de información.

5. Gestionar el plan

Una vez construido y aprobado el plan de continuidad la Entidad deberá emprender las acciones necesarias para comunicarlo a todos los empleados y contratistas de la entidad y de esta manera estar preparados para enfrentar situaciones de emergencia y restablecer en el menor tiempo posible el servicio, para lo cual se seguirá el siguiente protocolo:

1. Declaración manifiesta de la emergencia	Subproceso Gestión De Soporte y Apoyo Informático.
2. Informar Jefe del Proceso	Jefe Administrativo Financiero y Comercial
3. Contactar centro de operación (propio o alterno)	Reunión
4. Analizar daños (lista de chequeo)	Informe
5. Restablecimiento	Subproceso Gestión De Soporte y Apoyo Informático.
6. Mejora	Jefe Administrativo Financiero y Comercial

5.1. Normatividad asociada al Plan

- ISO/IEC 27001- Seguridad de la Información.
- ISO/IEC 27031- Guía para la preparación de las Tecnologías de Información y Comunicaciones para la continuidad del Negocio
- ISO 22301- Gestión de la Continuidad de Negocio
- ISO 31000 – Gestión de Riesgo.

6. Riesgos asociados a la continuidad del negocio

La EISCUCUTA SA E.S.P contempla implícitamente en la gestión de sus procesos la identificación y administración de los riesgos como práctica para impedir que eventualidades internas o externas impidan cumplir sus objetivos institucionales, por lo cual, al desarrollar el plan de continuidad del negocio se integra la metodología de riesgos aplicada y el control preventivo, defectivo y correctivo de dicho plan queda asociado al mapa de riesgos institucional.

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

IMPACTO	VALOR			
CATASTRÓFICO	20	20 **Zona de riesgo moderado** * Reducir el riesgo: Proteger la entidad * Compartir	40 **Zona de riesgo importante** * Reducir el riesgo: Prevenir el riesgo o Proteger la entidad * Compartir	60 **Zona de riesgo inaceptable** * Evitar el riesgo * Reducir el riesgo: Prevenir el riesgo o Proteger la entidad * Compartir
MODERADO	10	10 **Zona de riesgo tolerable** * Reducir el riesgo: Proteger la entidad * Compartir	20 **Zona de riesgo moderado** * Reducir el riesgo: Prevenir el riesgo o Proteger la entidad * Compartir	30 **Zona de riesgo importante** * Reducir el riesgo: Prevenir el riesgo o Proteger la entidad * Compartir
LEVE	5	5 **Zona de riesgo aceptable** * Asumir el riesgo	10 **Zona de riesgo tolerable** * Reducir el riesgo: Prevenir el riesgo	15 **Zona de riesgo moderado** * Reducir el riesgo: Prevenir el riesgo
PROBABILIDAD		BAJA	MEDIA	ALTA
VALOR		1	2	3

4

MAPA DE RIESGOS

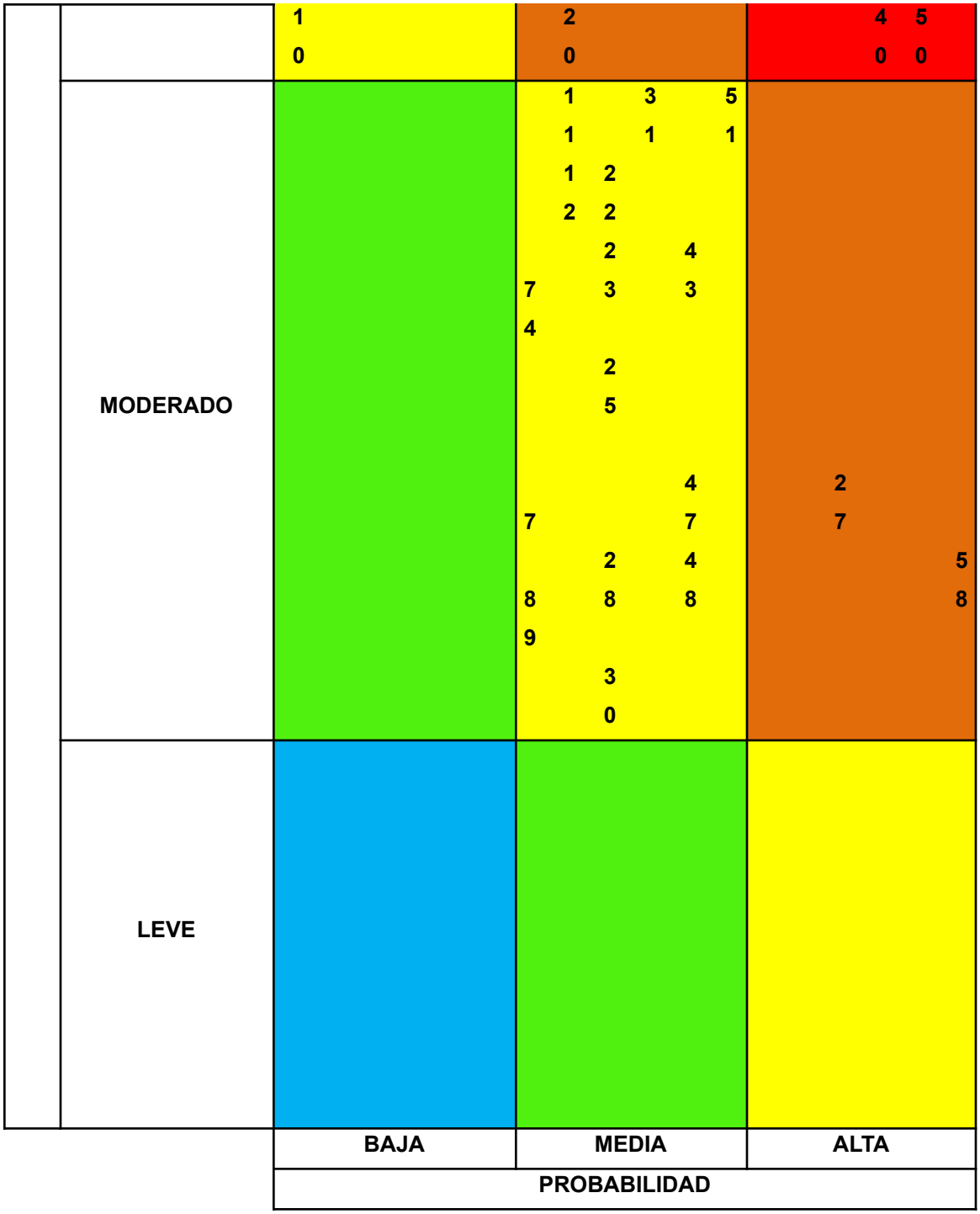
(1) SUBPROCESO	(2) COD.	(3) RIESGO	RIESGO INHERENTE			RIESGO RESIDUAL			
			(10) PROBABILIDAD	(12) IMPACTO	(13) GRADO DE EXPOSICIÓN	(19) PROBABILIDAD	(21) IMPACTO	RESULTADO	(22) GRADO DE EXPOSICIÓN
Gestión de Soporte y Apoyo Informático	54	ataques informaticos	ALTA	CATASTROFICO	ZONA DE RIESGO INACEPTABLE	MEDIA	MODERADO	MODERADOMEDIA	ZONA DE RIESGO MODERADO
Gestión de Soporte y Apoyo Informático	55	Interrupción parcial o total de los servicios tecnológico que afecte la Disponibilidad de la Información	MEDIA	CATASTROFICO	ZONA DE RIESGO IMPORTANTE	MEDIA	LEVE	LEVEMEDIA	ZONA DE RIESGO TOLERABLE
Gestión de Soporte y Apoyo Informático	56	Pérdida total o parcial de información	MEDIA	CATASTROFICO	ZONA DE RIESGO IMPORTANTE	MEDIA	MODERADO	MODERADOMEDIA	ZONA DE RIESGO MODERADO

Gestión de Soporte y Apoyo Informático	57	Afectación de la Integridad de la información	ALTA	CATASTROFICO	ZONA DE RIESGO INACEPTABLE	MEDIA	MODERADO	MODERADOMEDIA	ZONA DE RIESGO MODERADO
Gestión de Soporte y Apoyo Informático	58	Desactualización de tecnología computacional(infraestructura tecnológica)	ALTA	MODERADO	ZONA DE RIESGO IMPORTANTE	MEDIA	MODERADO	MODERADOMEDIA	ZONA DE RIESGO MODERADO

MAPA DE RIESGOS INHERENTE

ANTES DE IMPLEMENTAR CONTROLES

IMPACTO	**CATASTROFICO**	41, 2, 32, 42, 13, 33, 53, 34, 5, 35, 26, 37, 29	1, 21, 24, 44, 15, 45, 55, 16, 1, 46, 56, 19	52, 14, 54, 6, 17, 57, 18, 38, 39, 49



7. Roles y Responsabilidades

Rol	Responsable	Mecanismos
Documentador del Plan de continuidad.	Asesor SIG Representante Legal Jefe Del Proceso Líder del SUBPROCESO	Revisión del documento y aprobación y creación. Revisión y Firma

8. Desarrollo de las estrategias de Continuidad de TI

Aquí se desarrollará las estrategias definidas y se documenta el plan de recuperación como respuesta a un incidente o evento de TI que genere interrupción de los servicios soportados por TI.

9. Plan de Capacitación, Comunicaciones y Sensibilización de Seguridad y Privacidad de la Información.

La EISCUCUTA SA E.S.P debe definir un Plan de comunicación, sensibilización que incluya la estrategia para que la seguridad de la información se convierta en cultura institucional, al generar competencias y costumbres, para estructurar dicho plan se toma como base la Guía *No 14 – Plan de Comunicación, Sensibilización y Capacitación-min tic.*

10. Evaluación de Impactos Operacionales

Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad. El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

Nivel A: La operación es crítica para la entidad. Una operación es crítica cuando al no contar con ésta, la actividad no puede realizarse.
Nivel B: La operación es una parte integral de la Entidad, sin ésta la entidad no podría operar normalmente, pero la función no es crítica.
Nivel C: La operación no es una parte integral del Entidad.

Categoría	Proceso	Nivel	Tolerancia	Descripción
Aplicaciones	Sistema documentos	B	3	Contenedor de aplicaciones
Web	Sitio web Entidad	A	1	Capa de presentación
Base de Datos	SIEP TNS NOMINA	A	1	Contenedor de aplicaciones
Seguridad de Información	Firewall	A	1	Servicio de firewall de la Entidad
Almacenamiento	NAS	A	3	Dispositivo de Almacenamiento, con conexión al red, encargado de las copias de seguridad del sistema.
Comunicaciones	Internet	B	3	Comunicación internet local
Cuarto Técnico	Centro de Datos	A	1	Servicio de CD de la entidad
Proveedores de Aplicaciones,	Interno/externo	B	2	Desarrollo interno o contratado

comunicaciones y servicios				
Recurso Humano	Interno/externo	A	3	Profesionales encargados de administrar.

Tabla 1. Valoración Operacional por niveles de criticidad

10.1. Identificación de Procesos Críticos

La identificación de los procesos críticos de la entidad se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla.

Valor	Interpretación del proceso crítico
A	Crítico para la entidad. No se puede realizar
B	No es crítico, pero la operación es una parte integral del mismo.
C	La operación no es parte integral.

Tabla 2. Identificación de procesos críticos

10.2. Establecimiento de Tiempos de Recuperación

Una vez identificados los procesos críticos, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios.

Tiempo de Recuperación	Descripción
RPO***(Recovery Point Objective)***	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO ***(Recovery Time Objective)***	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.

WRT *(Work Recovery Time*)	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD *(Máximum Tolerable Downtime)*	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Tabla 3. Descripción de tiempos de recuperación

categoría	Proceso Critico	MTD (en días)	Prioridad de Recuperación
Aplicaciones	Flujo de documentos	3 días	3
Aplicaciones	SIEP Error	2 días	1
Aplicaciones	SIEP Desarrollo Nuevo	Depende de lo que la entidad requiera se hace una estimación y se cotiza. Y se hace un comité de cambio, para saber qué tiempo se gastaría en el nuevo desarrollo.	1
Seguridad de Información	Firewall	0.5 día*	1
Sistemas de Almacenamiento	NAS	3 HORAS	1
Comunicaciones	Servicio Wifi, conexión internet	Continuidad por el Proveedor	2
Cuartos de Máquinas	Centro de Datos	0.5 día*	1

Soporte Informático	Equipo PC de usuario	3 días	4
Hosting	Almacenamiento	Continuidad Proveedor-administrable por contratista de la entidad.	2
Plataforma de Correos	Servicio de Correo	Continuidad Proveedor-administrable por contratista de la entidad.	1

*: Corresponde al tiempo de inactividad del proceso crítico del negocio, que tomaría menos de un (1) día de tolerancia de inactividad del servicio.

10.3. Continuidad Del Servicio Conexión Internet

El servicio de conexión depende del prestador del servicio CLARO, en el cual la empresa es un cliente corporativo. El procedimiento a seguir en la indisponibilidad del servicio comenzará a contar a partir de recibir el reporte de la falla en el servicio en nuestro centro de Soporte al Usuario mediante un numero de PQR.
Claro Ofrece un soporte de:

7X24

La indisponibilidad terminará en el momento en que la falla sea solucionada.

Además de que la entidad cuenta con E-Care es una práctica herramienta desarrollada, para facilitar la interrelación, consulta, administración y soporte de los servicios contratados con claro. Esta plataforma permite la autogestión en línea donde permite:

Acceder a la información desde cualquier parte del mundo vía Internet

- Seguridad y Privacidad a través de un único login y password por cliente
- Gestionar tickets Técnicos
- Ver la información de sus servicios
- Obtener la información de facturación del último año
- Ver el detalle gráfico de su solución
- Gestionar su usuario.

TIEMPO DE ATENCION DE FALLAS:

NIVEL (PRIORIDAD) DE LA FALLA	EFECTO DE LA FALLA	TIEMPO MAXIMO DE ATENCION
1	DESCONEXION TOTAL	1 HORA
2	OPERACIÓN DENEGADA	2 HORAS
3	FALLA NO GRAVE	3 HORAS

SOPORTE TECNICO Y MANTENIMIENTO: Soporte Corporativo

Nivel	Cantidad Contactos
NIVEL 1	1
NIVEL 2	1
NIVEL 3	1

NIVEL 4	1

El servicio ofertado en nuestra solución es 7 X 365 X 24. Se escala a 4 niveles ofrecidos por CLARO corporativo una vez hecho la solicitud y generado el ticket.

HORARIO DE ATENCION AL SOPORTE TECNICO:

LUNES A VIERNES	**8:00 am – 12:00 m , 2:00 pm – 6:00 pm**
SABADOS	**8:00 am – 12:00 m , 2:00 pm – 6:00 pm**
DOMINGOS Y FESTIVOS	**9:00 am – 12:00 m**

10.4. Soporte Siep

Además la entidad cuenta con el soporte técnico y/o remoto permanente e inmediato a los usuarios finales, de los distintos módulos del SIEP., cada vez que se requiera, solucionando problemas de infraestructura tecnológica en lo relacionado con el software.

HORARIO DE ATENCION AL SOPORTE TECNICO:

LUNES A VIERNES	**8:00 am – 12:00 m , 2:00 pm – 6:00 pm**
SABADOS	**8:00 am – 12:00 m , 2:00 pm – 6:00 pm**

10.5. Soporte Hosting

El plan adquirido por la empresa es Rubí Empresarial el cual nos ofrece soporte de las siguientes maneras:

- Email: soporte@dongee.com
- Chat: en nuestro sitio web www.dongee.com
- WhatsApp: Añadiendo el número +13058901818
- Facebook Messenger.
- Base de conocimiento: soporte.dongee.com
- Teléfonos: disponibles en la parte superior de nuestro sitio web (arriba a la derecha) https://www.dongee.com
- Voice to ticket. Deje un mensaje de voz con sus datos y devolvemos la llamada
- Telegram: Cuenta @dongee_bot
- Twitter: Enviando un mensaje directo en @dongeehost en https://twitter.com/messages/compose
- Line.

- Tiempo de Respuesta promedio es de 2 minutos, sin embargo, todos los eventos críticos o incidentes están conectados a nuestro monitoreo integrado a notificaciones y se ejecuta cada 30 segundos. En ese momento un ingeniero Nivel 2 ingresa a verificar y resolver el incidente. La prioridad es en la resolución de la situación y posteriormente otros ingenieros podrán responder cualquier mensaje recibido a través de nuestros canales.
- Cada 30 segundos todo el hardware y software de la plataforma está siendo monitoreado. si se presenta un incidente en datacenter un ingeniero se desplaza hasta el hardware y toma medidas al respecto para resolver cualquier problema en él. Estas notificaciones llegan también a nuestro staff de soporte para resolver inmediatamente cualquier incidente. Normalmente entre el tiempo de la incidencia y la solución llegan muy rápido.
- En momentos que toma reparar algo extenso, por ejemplo un crash en un motor de bases de datos, el ingeniero se concentra en resolver el incidente para tener el RTO más bajo posible.

- Dongee cuenta con un servicio de monitoreo de carga que permite enviar un mensaje a nuestra plataforma de comunicación interna del staff de soporte si un sitio web se demora más de 12 segundos y un miembro del staff ingresa a tomar control de la situación de inmediato. De esta manera se garantiza que el sitio cargue siempre rápido en la mayor parte del tiempo. Estos chequeos se realizan cada 3 minutos.
- Existe un momento especial que es desde las 10 pm a 4 am de la mañana en donde día de por medio se realizan backups a nivel de disco que puede afectar el rendimiento, haciendo que el sitio cargue no con el promedio sino sumando de 2 a 5 segundos de carga. Pero sin causar la caída de los mismos.

10.6. Soporte Remoto

La entidad cuenta con el soporte técnico y/o remoto en horarios laborales e inmediato a los usuarios finales, por parte del personal contratado., cada vez que se requiera, solucionando problemas de infraestructura tecnológica en lo relacionado con el software.

10.7. Backups

Software para realizar copias de seguridad de las máquinas virtuales que soportan los procesos operativos de la organización, esta copia se realiza a nivel de toda la máquina, con su sistema operativo, aplicaciones, configuraciones especiales además de los datos.

El proceso de copias se realiza de forma segura, es decir la información se encripta antes de ser enviada y almacenada en el servidor destino

ERVIDOR PRINCIPAL	***MAQUINAS VIRTUALES***	***POLITICAS DE RESPALDO***	***POLITICA RETENCION***	***UBICACIÓN***

SERVIDOR EIS	TNS,SIEP Y ACCESOS REMOTOS	L-V 00:00 L-V 09:00 L-V 12:00 L-V 15:00 L-V 18:00 S-D 00:00 S-D 12:00	2 SEMANAS	NAKVIO
SERVIDOR EIS	MV PBX	L-V 00:00 L-V 08:00 L-V 11:00 L-V 14:00 L-V 17:00 S-D 00:00 S-D 12:00	2 SEMANAS	NAKVIO

10.8. Restauración

La restauración de los sistemas, se hace a través de NAKIVO con una IP asignada, se ingresan los datos de usuario, y se siguen los siguientes pasos en el DASHBOARD:

- Se listan los backups de las máquinas virtuales.
- Se selecciona la máquina virtual a restaurar.
- Se escoge la máquina se selecciona la opción recover, en donde hay varios modos de restauración pero por lo general se optara por una restauración completa VM recovery from backup que restaura el estado completo de la MV a un punto específico. Esto puede tardar unas tres horas.

11. Estrategia De Vuelta A La Normalidad

Esta fase consiste en retornar la operación a la normalidad después de activar el PCN y haber superado el evento que lo activo. Por lo que se tendrá que verificar, al momento del retorno, que la sincronía entre los datos y los mismos sean correctos y confiables.

Teniendo en cuenta las estrategias establecidas, se determinará el plan de retorno para cada una de ellas.

ESCENARIO	ESTRATEGIA
1. Imposibilidad de Acceso a sitio normal de trabajo (Edificio San José)	Trabajo Remoto o Teletrabajo (acceso remoto a través de una IP, usuario y contraseña, los usuarios se pueden conectar remotamente)
2. Falla de la tecnología (Centro de datos local)	Backup / Restore
3. Ausencia de Personal	Backup de Roles críticos
	Documentación de procesos críticos
4. Falla en proveedor de tecnología (canal de comunicación)	Acuerdo con diferentes proveedores

Conclusiones

implementar un Plan de Continuidad de Negocios para amortiguar y minimizar los efectos de la contingencia críticos, operativos y financieros, reduciendo el tiempo en la recuperación de la información, restaurando los procesos operacionales clave de sus recursos y servicios de TI, ocasionadas por fallas, desastres naturales, siniestros, e incluso epidemias.

VIANNY KARINA BUITRAGO Apoyo de gestión de soporte informático	**RAFAEL TAMAYO VILLAMIZAR** Líder SIG	**CARLOS JOSÉ IBARRA RODRÍGUEZ** Representante De la Dirección
Fecha	Fecha:	Fecha: