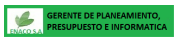
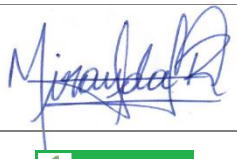
ENACO S.A.
EMPRESA NACIONAL DE LA COCA S.A.

Código: PL-S2-001	Versión: 00

Plan Interno: "Plan de Contingencias Informático"

Julio 2020

	CARGO	FIRMA
Elaborado por:	**Coordinador de Tecnologías de la Información y Comunicaciones**	
Revisado por:	**Gerente de Planeamiento, Presupuesto e Informático**	 GERENTE DE PLANEAMIENTO, PRESUPUESTO E INFORMATICA Firmado digitalmente por: GALARZA MESIAS Cristian Eduardo FAU 20114883230 hard Fecha y hora: 06.08.2020 22:03:00
Homologado por:	**Analista de Planeamiento**	
Aprobado por:	**Gerente General (e)**	 GERENTE GENERAL (e) Firmado digitalmente por: GALARZA MESIAS Cristian Eduardo FAU 20114883230 hard Fecha y hora: 06.08.2020 22:00:05

Control de Cambios			
Fecha	**Versión**	**Sección / Ítem**	**Descripción del cambio:**
Julio 2020	00		

1. GENERALIDADES

1.1. Objetivos

Los objetivos que se persigue en el presente plan son los siguientes:

- Se deben definir las actividades de planeación, preparación, capacitación y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.
- Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

1.2. Finalidad

Disponer de un plan que permita atender de manera ordenada y prevista situaciones que pongan en riesgo la operatividad de los Sistemas Informáticos y de Redes en la Empresa Nacional de la Coca; estableciendo procedimientos que eviten interrupciones en su operación.

1.3. Base legal

- Ley N° 27658 - Ley Marco de Modernización de la Gestión del Estado.
- Ley N" 23716 - Ley de Control Interno de las Entidades del Estado.
- Resolución de Contraloría General N° 320-2006-CG, aprueba las Normas de Control Interno del Sector Publico.
- Guía Práctica para el desarrollo de planes de contingencia de sistemas de información – INEI.
- Resolución Ministerial N° 028-2015-PCM, Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- Resolución Ministerial N° 004-2016-PCM, aprueban el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema a Nacional de Informática

1.4. Alcance

El Plan de Contingencia de los Sistemas de Información de ENACO está diseñado para crear una situación de preparación que proporcione una respuesta inmediata diseñada en función de una serie de posibles escenarios previamente definidos.

1.5. Definiciones

- **Copias de Seguridad (Backup)**: una copia de seguridad o backup (su nombre en inglés) en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.
- **Disco Duro**: en informática, un disco duro o disco rígido (en inglés Hard Disk Drive,

HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.

- **Enrutador (Rourter)**: el enrutador (calco del inglés Router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.
- **Hardware**: corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
- **LAN**: (Local Área Network - Red de Área Local). Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.
- **Plan de Contingencia**: Conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas, dentro de unos límites de tiempo establecidos. Sin que sea una regla general, se suele aplicar al plan circunscrito a las actividades de los departamentos de Sistemas de Información.
- **Red**: Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información.
- **Software**: se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.
- **Servidores**: una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.
- **S.O. (Sistema Operativo)**: un Sistema operativo (SO) es un software que actúa de interfaz entre los dispositivos de hardware y los programas de usuario o el usuario

mismo para utilizar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como intermediario para las aplicaciones que se ejecutan.

- **Servidor Espejo**: con ese nombre se conoce a un procedimiento de protección de datos y de acceso a los mismos en los equipos informáticos.

2. MARCO METODOLÓGICO

El presente Plan de Contingencia ha sido elaborado tomando como base las fases definidas en "Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de información" publicada por el INE1. Es a partir de esta guía que son adoptadas las siguientes fases y son detalladas a continuación:

a. Identificación de riesgos.

b. Estrategias para la recuperación de desastre, incidencia o evento.

c. Realización de pruebas (implementación).

Las escalas a utilizar en el presente documento corresponden a:

Escala cualitativa de probabilidades.

Constituye la representación de escalas descriptivas para demostrar la magnitud de consecuencias potenciales y su posibilidad de ocurrencia. Para cada riesgo identificado se evalúan los niveles de probabilidad e impacto.

CATEGORIA	DEFINICIÓN
ALTO	Es muy probable la materialización del riesgo o se presume que llegará a materializarse.
MEDIO	Es probable la materialización del riesgo o se presume que posiblemente se podrá materializar
BAJO	Es poco probable la materialización del riesgo o se presume que no llegará a materializarse.

Escala cuantitativa de impacto.
El mismo diseño definido para la escala cualitativa es empleado para la escala cuantitativa, la cual es detallada a continuación:

CATEGORIA	DEFINICIÓN
ALTO	Si el hecho llegará a presentarse, se tendría alto impacto o efecto sobre la entidad.
MEDIO	Si el hecho llegará a presentarse, se tendría media impacto o efecto sobre la entidad
BAJO	Si el hecho llegará a presentarse, se tendría bajo impacto o efecto sobre la entidad.

Escalas cuantitativas de probabilidad e impacto.
A continuación, son descritas las escalas cuantitativas de probabilidad e impacto:

PROBABILIDAD DE OCURRENCIA	NIVEL
1	BAJO
2	MEDIO
3	ALTO

IMPACTO	NIVEL
1	BAJO
2	MEDIO
3	ALTO

Evaluación y clasificación de riesgo

			POBABILIDAD		
			1	2	3
			BAJO	MEDIO	ALTO
IMPACTO	3	ALTO	(3) Riesgo Moderado	(6) Riesgo Importante	(9) Riesgo Inaceptable
	2	MEDIO	(2) Riesgo Tolerante	(4) Riesgo Moderado	(6) Riesgo Importante
	1	BAJO	(1) Riesgo Aceptable	(2) Riesgo Tolerante	(3) Riesgo Moderado

Niveles de Riesgo

Nivel de Riesgo (Cualitativo)	Nivel de Riesgo (Cuantitativo)	Prioridad	Descripción
Riesgo Inaceptable	9	Muy Alta	Se requiere acción inmediata, planes de tratamiento requeridos, implementados y reportados a la alta dirección.
Riesgo Importante	6	Alta	Se requieren planes de tratamiento requeridos, implementados y reportados a los jefes de las oficinas, direcciones entre otros.

Nivel de Riesgo (Cualitativo)	Nivel de Riesgo (Cuantitativo)	Prioridad	Descripción
Riesgo Moderado	3 y 4	Medio	Debe ser administrado con procedimientos normales de control.
Riesgo Tolerante	2	Baja	Menores efectos que pueden ser fácilmente remediados, se administran con procedimientos rutinarios.
Riesgo Aceptable	1	Muy Baja	Riesgo insignificante. No se requiere ninguna acción.

Cuantificación de Riesgos

Los riesgos serán cuantificados de acuerdo a dos factores:

Probabilidad, que representa la posibilidad de que se presente el desastre, incidencia o evento.

Impacto, representa la envergadura del riesgo, es decir cuánto puede afectar.

RIESGO = PROBABILIDAD X IMPACTO

2.1. Identificación de riesgos

2.1.1. Análisis de riesgo.

La empresa está expuesta a riesgos que pueden ser causados por eventos fortuitos o por el mal uso de los recursos, pudiendo afectar los objetivos o las metas trazadas por la empresa. En ese sentido, la identificación de los riesgos se encuentra referidos a aquellos que afectan la seguridad del centro de datos, el cual trae como consecuencia la indisponibilidad, y afecta la operación y continuidad de los servicios.

2.1.2. Relación de riesgos que pueden afectar l centro de datos

A continuación, son detallados riesgos identificados at centro de datos de ENACO y se describen a continuación:

#	Riesgo Identificado	Descripción del riesgo	Consecuencia
1	Terremoto	Fenómeno natural manifestado por una sacudida brusca de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas sísmicas.	Destrucción del ambiente destinado para el centro de datos, generando la interrupción de todos los servicios que brinda.

#	Riesgo Identificado	Descripción del riesgo	Consecuencia
2	Inundación / aniego.	Ocupación de agua en zonas que habitualmente están libres debido al desbordamiento de ríos, torrentes, lluvias torrenciales, deshielo, por subida de las mareas por encima del nivel habitual, por maremotos entre otros.	Equipos inservibles por el ingreso de agua al ambiente destinado para el centro de datos, generando la interrupción de todos los servicios que brinda.
3	Incendio.	Ocurrencia de fuego no controlado que puede afectar los bienes.	Destrucción del ambiente destinado para el centro de datos, generando la interrupción de todos los servicios que brinda.
4	Vandalismo.	Se refiere a atentados que podrían afectar o destruir las instalaciones, equipos, programas informáticos, datos, documentación y el ministerio, por su función está expuesto a ser afectado.	Interrupción parcial o total de los servicios que brinda el centro de datos.
5	Fraude.	Evento referido a la alteración o sustracción de datos para uso en contra de la institución o en beneficio del autor del acto.	Uso ilícito de los recursos de la Empresa en contra de la institución.
6	Intrusión de la red.	Ataques que provienen localmente o de Internet, originados por hackers, virus con la finalidad de alterar el normal funcionamiento de los recursos informáticos.	Interrupción parcial o total de los servicios que brinda el centro de datos.
7	Falta de fluido Eléctrico.	Pérdida del suministro eléctrico en el centro de datos.	Perdida del suministro de energía eléctrica en el centro de datos, pudiendo originar daño en los equipos sensibles, perdida de información originando una interrupción en los servicios que brinda el centro de datos

2.1.3.Cuantificación de los riesgos identificados

En el siguiente cuadro se detallan la clasificación de los riesgos identificados en atención a lo señalado en la metodología definida.

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
1	Terremoto	2	3	6	Riesgo Importante
2	Inundación / aniego.	1	3	3	Riesgo Moderado
3	Incendio.	1	3	3	Riesgo Moderado

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
4	Vandalismo.	1	2	2	Baja
5	Fraude.	1	2	2	Baja
6	Intrusión de la red.	2	2	4	Riesgo Moderado
7	Falta de fluido Eléctrico.	2	3	6	Riesgo Importante

De la valoración realizada en la matriz probabilidad por impacto, se ha identificado que existen riesgos cuyo nivel han sido valorados como importante y moderado según la probabilidad y el impacto que estos podrán generar en el centro de datos de producirse.

En ese sentido, concluimos que el análisis evidencia las posibles contingencias que pudieran presentarse y afectar a los sistemas de información y la plataforma que permite su operación, para lo cual el presente "PLAN DE CONTINGENCIA" desarrollara las estrategias a fin de poder mitigar los RIESGOS IMPORTANTES y RIESGOS MODERADOS identificados

2.2. Estrategia para la recuperación de desastres

La generalización del uso de los medios electrónicos, informáticos y telemáticos supone beneficios, pero también riesgos asociados ante la ocurrencia de un desastre, incidente o evento por lo que se debe mitigar su impacto non acciones que permitan dar continuidad de los servicios de TI, por Ío que son definidas acciones antes (preventivas), durante y después (reactivas)

2.2.1. Actividades previas al desastre (Preventiva)

Son aquellas actividades de planeamiento, preparación, entrenamiento y ejecución de las acciones de resguardo de información que nos permita un proceso de recuperación viable de los servicios de TI proporcionados por el centro de datos de ENACO. En ese sentido, se hace necesario el contar con la siguiente información:

2.2.1.1. Sistemas de Información

El área de Tecnología de Información de ENACO deberá contar con una relación de los Sistemas de Información (anexo 1); dicha relación debe considerar la siguiente información:

- Nombre de la aplicación o Sistema.
- Lenguaje con el que fue creado el Sistema, incluyendo la relación de librarías que lo conforman.
- Área usuaria, esto es el área usuaria dueña del proceso sistematizado.
- Las unidades orgánicas y entidades (internos/ externos) que usan la

información del Sistema.

- El volumen de los archivos (en MB) que trabaja el Sistema, si fuera el caso.
- El Tamaño de la base de datos (en MB).
- La(s) fecha(s) criticas, en las que la información es necesaria y debe estar disponible.

2.2.1.2. Hardware del centro de datos

- El área de Informática OIST deberá inventariar los servidores y PCs de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.
- Alta disponibilidad de hardware del centro de datos; El centro de datos principal ubicado en la Sede administrativa, contará con un centro de datos alterno a nivel de hardware y software en la Sede Comercial Cusco, permitiendo la continuidad de negocio, en este caso se probará y asegurará que los procesos de restauración de información posibiliten el funcionamiento adecuado de los sistemas

2.2.1.3. Respaldo de la información (Backups)

Establecer los procedimientos (políticas o procedimientos de backup determinando responsabilidades en la obtención de los Backups críticos identificados) para la obtención de copias de seguridad necesarios para asegurar la disponibilidad de la información para la correcta ejecución de los sistemas o aplicativos ante la ocurrencia de un desastre, incidente o evento tales como:

- Archivos de configuración de aplicativos
- Código fuente de aplicativos
- Documentos adjuntos de aplicativos
- Archivos de unidades compartidas
- Motor de Base de datos
- Software base de PCs y Servidores

2.2.1.4. Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

2.2.1.5. Formación de equipos de evaluación

Esta función debe ser realizada de preferencia por personal externo con experiencia en Seguridad de la Información, de no ser posible, la realizará el personal de la Gerencia de Planeamiento, Presupuesto e Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar el cumplimiento de las normas y/o procedimientos con respecto a Backups y seguridad de equipos y data.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de sistemas e informaciones necesarios para la buena marcha de la Empresa, y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las normas y/o procedimientos, para las acciones de corrección respectivas.

2.2.2.Actividades durante el desastre.

Una vez presentada la contingencia, es necesaria la participación de todas las personas del área donde ocurre la contingencia para lo cual se debe:

2.2.2.1. Plan de emergencias.

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, además deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan).
- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.).
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Policía Nacional del Perú y de su personal (equipos de seguridad) asignados para estos casos.
- Se debe seguir lo señalado en las fichas de contingencia para los casos identificados en el presente plan de contingencia (anexo 3)

2.2.2.2. Formación de equipos

El personal de área de Tecnología de la Información es el responsable del salvamento de equipos informáticos, de acuerdo a la clasificación de prioridades.

2.2.3.Actividades después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, para restaurar todos los servicios de TI y la operación de la empresa:

2.2.3.1. Evaluación de Daños

Inmediatamente después que el desastre, incidente o evento ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo de acuerdo a la matriz de probabilidad por impacto. Luego de la evaluación, se identificarán las actividades a ser desarrolladas a fin de restaurar los servicios de TI afectados para lo cual se deberá tomar como referencia las actividades descritas en las fichas de contingencia identificadas (anexo 3).

2.2.3.2. Priorización de Actividades

Si el siniestro es general y contempla una pérdida total; la evaluación de daños reales y su comparación contra el plan, proporcionará la lista de las actividades a realizar en función de la prioridad.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, a fin de asignarlos en forma temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

2.2.3.3. Ejecución de Actividades

Las actividades identificadas y priorizadas para la recuperación de ocurrido el desastre, incidente o evento, deberán ser realizadas por los equipos de trabajo y se contará con un coordinador que reportará el avance de los trabajos de recuperación al encargado del Plan de Contingencias. Las actividades de recuperación serán en dos etapas:

- La primera, la restauración de los servicios priorizados de TI del centro de datos.
- La segunda, es volver a contar con todos los servicios y los recursos informáticos, debiendo ser esta última etapa lo suficientemente rápida y eficiente en la medida de lo posible.

2.2.3.4. Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los servicios de TI que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades de recuperación de los servicios, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de

recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro

2.2.3.5. Retroalimentación

Con la evaluación de resultados, debemos de optimizar el Plan de Contingencia original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente

2.3. Realizar pruebas de implementación

El equipo operativo será conformado por los colaboradores que designe el Área de TI y el oficial de seguridad de la información, esto con la finalidad de realizar las pruebas antes de ocurrir un desastre, incidente o evento ocurra. Las actividades que serán realizadas corresponden a:

- Supervisar los procedimientos de respaldo y restauración de los sistemas de información.
- Participar en las pruebas y simulacros de desastres.
- Contar con un listado de personas que serán contactadas de ocurrir un desastre (anexo 2).

3. Disposiciones finales

- El Plan de Contingencias de TI deberá contar con el apoyo correspondiente por parte de la Alta Dirección, para suministrar de recursos financieros y humanos a fin de su implementación y ejecución.
- Realizar la conformación de un Comité el encargado de planificar, implementar y supervisar la ejecución del Plan de Contingencia, que asegure la legalidad, consistencia, adecuado uso, seguridad, inviolabilidad y sostenibilidad de los Sistemas de Información, hardware y software.
- La actualización del presente plan de contingencia debe ser realizado una vez al año.
- Todos los colaboradores que laboren en el Área de TI, deben formar parte de las actividades y están obligados a participar en la implementación y ejecución del Plan de Contingencias de TI.
- Definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento del Plan de Contingencia.
- Las medidas que debemos adoptar para protegernos son tantas como amenazas existen, es por ello que se debe difundir a todas las unidades operativas de ENACO el presente plan de contingencia.
- Realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Plan de Contingencia.
- Contar con un centro de datos alterno a fin de minimizar el tiempo de recuperación de los servicios de TI.
- Se debe prever contar con un sistema de respaldo eléctrico (UPS más banco de baterías)

exclusivo para ambos centros de datos; y que la trasferencia de energía sea de manera automática.

ANEXO 1

ELACIÓN DE LOS SISTEMAS DE INFORMACIÓN Y SU BASE DE DATOS EN PRODUCCIÓN

NOMBRE CORTO	DESCRIPCIÓN	TECNOLOGIA	GESTOR DE BASES DE DATOS	UBICACIÓN DE BASE DE DATOS	HERRAMIENTA DE DESARROLLO	SITUACIÓN
SIE	Sistema de Información de ENACO, que incluye los módulos de Ventas, Compras, Inventarios, Contabilidad, Logistica, RRHH, Tesorería, Presupuesto y Patrimonio; para las operaciones de la Empresa.	Cliente/Servidor	MS SQL Server 2008	IBM X 3550 M3; Microsoft Windows Server 2008 R2, SP1.	Visual FoxPro	En producción
TDE	Sistema de Trámite Documentario ENACO, donde se gestiona los distintos tipos de documentos en los procesos internos de la Empresa.	Web	PostgreSQL 9.4	IBM X 3550 M3; Microsoft Windows Server 2008 R2, SP1.	PHP 5.2.4.	En producción
LEGAJOS	Aplicación de File de Personal, contiene los módulos de INGRESO DE DOCUMENTOS ESCANEADOS, CLASIFICACION y CONSULTAS	Cliente/Servidor	MS SQL Server 2008	IBM X 3550 M3; Microsoft Windows Server 2008 R2, SP1.	Visual Studio .NET	En producción

NOMBRE CORTO	DESCRIPCIÓN	TECNOLOGIA	GESTOR DE BASES DE DATOS	UBICACIÓN DE BASE DE DATOS	HERRAMIENTA DE DESARROLLO	SITUACIÓN
PÁGINA WEB INSTITUCIONAL.	Página Web de ENACO	Web	MySQL	IBM X 3550 M3; Microsoft Windows Server 2008 R2, SP1.	WordPress 5.2.5	En producción
GOOGLE G-SUITE	Servicio de correo corporativo y herramientas colaborativas de comunicación de ENACO	Nube				En producción
REPORTE COCALEROS	Consulta WEB para los productores de las ventas de hoja de coca que realizaron a la empresa ENACO	Web	MySQL	IBM X 3550 M3; Microsoft Windows Server 2008 R2, SP1.	Net Beans 8.2	En producción
COE	Registro controles operativos policiales realizados por la Supervisión de Fiscalización.	Web	PostgreSQL 9.4		PHP 5.2.4.	En producción
INTRANET	Gestionas las Directivas (Vigentes Y Prorrogadas)	Web	MySQL	IBM X 3550 M3; Microsoft Windows Server 2008 R2, SP1.	WordPress 5.2.5	En producción

NOMBRE CORTO	DESCRIPCIÓN	TECNOLOGIA	GESTOR DE BASES DE DATOS	UBICACIÓN DE BASE DE DATOS	HERRAMIENTA DE DESARROLLO	SITUACIÓN
SISTEMA DE ARCHIVO WEB	Permite contar con un sistema que aloje en formato electrónico todos los documentos físicos que se encuentra en el área de archivo, para una mejor gestión y disponibilidad de los mismos.	Web	SQL Server 2012	Tercero	Visual Studio .NET	En producción
SISTEMA DE TRACKING Y MANTENIMIENTOS VEHICULARES	Permite a los usuarios de la contar con un aplicativo que monitorea las unidades vehiculares y gestione los mantenimientos.	Web	Tercero	Tercero	Tercero	En producción
Web de Compras de Hoja de Coca	ENACO contará con un aplicativo de compras de hoja de coca en cualquier punto con o sin Internet, el mismo que se integrará en el actual ERP SIE.	Web	Tercero	Tercero	Tercero	En Desarrollo

ANEXO 2

DESCRIPCIÓN DE EQUIPOS DE TRABAJOS

COORDINACIÓN: EQUIPO DE RESPUESTA A EMERGENCIA EN EL CENTRO DE DATOS

Nro	Nombre de Personal	Cargo	Celular/Teléfono
01		Coordinador de Tecnologías de la Información y Comunicaciones	943688387
02		Oficial de Seguridad de la Información	963766772
03		Gerente de Presupuesto, Planificación e Informático	989223556

LISTADO DE PERSONAL: EQUIPO DE RESPUESTA DE EMERGENCIA DE SEGURIDAD PERIMETRAL

Nro	Nombre de Personal	Cargo	Celular/Teléfono
01		Coordinador de Tecnologías de la Información y Comunicaciones	943688387
02		Asistente de Soporte Técnico	943789745
03		Gerente de Presupuesto, Planificación e Informático	989223556

LISTADO DE PERSONAL: EQUIPO DE RESPUESTA DE EMERGENCIA DEL CENTRO DE DATOS

Nro	Nombre de Personal	Cargo	Celular/Teléfono
01		Coordinador de Tecnologías de la Información y Comunicaciones	943688387
02		Analista Programador	984108718
03		Gerente de Presupuesto, Planificación e Informático	989223556

LISTA DE PROVEEDOR

Nro	Nombre de Personal	Proveedor	Celular/Teléfono
01			
02			
03			

ANEXO 3

DESCRIPCIÓN DE ACTIVIDADES POR TIPO DE RIESGO

RIESGO: INTRUSO

1. DESCRIPCIÓN DEL EVENTO

Ataques que provienen desde Internet, originales por hackers, virus con la finalidad de alterar el normal funcionamiento de los recursos

2. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.
2. Contar con los equipos de seguridad perimetral actualizados y con soporte vigente.
3. Contar con antivirus instalados en las PC y servidores, actualizados y con soporte vigente.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Verificar que se realicen respaldos de la información de manera periódica por la AST, debiendo generar la respectiva acta de evidencia.
2. Verificar se cuente con la actualización y el soporte vigente del IPS y el antivirus, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	CA	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Confirmada la presencia de una intrusión en la red, se deberá investigar su origen para lo cual se debe comprobar cuáles son los equipos y servicios que se están siendo comprometidos a fin de identificar los causantes del ataque.
2. Desconectar el o los equipos infectados de la red.

3. Visualizar los procesos activos en los servidores a fin de identificar comportamiento inusual en estos, debiendo considerar:
   a. Procesos que llevan activos un largo periodo de tiempo
   b. Procesos que consumen un nivel elevado de CPU
   c. Procesos que no están ejecutados desde una PC perteneciente a la red del ENACO
3. Revisar los archivos de registro (log) a fin de obtener información sobre conexiones a lugares poco frecuentes, utilización de aplicaciones inusuales y otras actividades sospechosas de intrusión.
4. Chequeo de los archivos del sistema a fin de detectar si han sido modificados.
5. Comprobar los puertos de conexión abiertos; a fin de detectar si hay alguno en especial que no lo debería ser.
6. Comprobar la existencia de sniffers en la red de ENACO

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Realizar el monitoreo del incidente.

4. ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades de recuperación (después)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. De detectarse que la incidencia ha afectado a algún componente de software o hardware del servidor, se debe comunicar al dueño de la información a fin de que verifique su impacto.
2. Si se comprueba que los equipos de seguridad han fallado en la detección de intrusos, debe recurrirse al proveedor a fin de comunicar el hecho.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo e informar al AST.
2. Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
3. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora ·continua) y actualizar las fichas de contingencia.

RIESGO: TERREMOTO

1. DESCRIPCIÓN DEL EVENTO

Fenómeno natural manifestado por una sacudida brusca de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas sísmicas.

2. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.
2. Asegurar que los elementos que se encuentran en el centro de datos sean ubicados de manera tal que permanezcan estables durante la contingencia y cumplan con el estándar para centro de datos
3. Se mantendrán cerradas las puertas de los gabinetes a fin de minimizar la caída de equipos u otros.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

2. Verificar se realicen respaldos de la información de manera periódica por el AST, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	IC	R	CA	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Evacuar el área si es necesario, utilizando las rutas de emergencia buscando un lugar seguro y evitando ventanas, así como el uso de escaleras.

4. ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD

ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades de recuperación (después)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
2. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si cuenta con la protección necesaria.
3. Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
3. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

RIESGO: INUNDACIÓN / ANIEGO

1. DESCRIPCIÓN DEL EVENTO

Ocupación de agua en zonas que habitualmente están libres debido al desbordamiento de ríos, torrentes, lluvias torrenciales, por subida de las mareas por encima del nivel habitual, por maremotos entre otros.

2. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Verificar se realicen respaldos de la información de manera periódica por el AST, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	A	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Evacuar el área, utilizando las rutas de emergencia de ser el caso
2. Únicamente si las brigadas y/o autoridades indiquen que es seguro, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado, de ser factible.

4. ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades de recuperación (después)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
2. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si cuenta con la protección necesaria.
3. Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
3. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

RIESGO: INCENDIO

1. DESCRIPCIÓN DEL EVENTO

Ocurrencia de fuego no controlado que puede afectar los bienes.

2. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Distribuir el área de Informática de tal forma que los equipos y dispositivos de mayor cuidado y valor sean colocados en lugares con menor riesgo y fácil evacuación.
2. Implementar extintores de hielo seco y recibir el entrenamiento necesario para su utilización.
3. Verificar las instalaciones eléctricas y reemplazar todos los toma corrientes defectuosos.
4. Verificar se realicen respaldos de la información de manera periódica por el AST, debiendo generar la respectiva acta de evidencia.

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Evacuar el área, utilizando las rutas de emergencia de ser el caso.
2. Uso de extintores para tratar de apagar el incendio
3. Alertar a los Bomberos, para ello se recurrirá a los números telefónicos de emergencia, a efectos de obtener una pronta respuesta al acontecimiento.
4. Evacuación de los equipos mas importantes, de mayor costo y de fácil movilidad.
5. Únicamente si existen las condiciones de seguridad, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado de ser factible.

4. ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades de recuperación (después)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
2. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si cuenta con la protección necesaria.
3. Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
3. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

RIESGO: FALTA DE FLUIDO ELÉCTRICO

1. DESCRIPCIÓN DEL EVENTO

Pérdida de electricidad a corto o largo plazo en una zona, y puede tener muchas causas, como fallos en una estación eléctrica, daños en las líneas de transmisión, subestaciones u otras partes del sistema de distribución, un cortocircuito o una sobrecarga de la alimentación eléctrica.

2. ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Realizar pruebas periódicas del sistema de abastecimiento eléctrico.
2. Realizar las configuraciones respectivas de fallas, caídas o problemas del UPS

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Proveer sistema eléctrico de abastecimiento (UPS + banco de baterías) independiente en el centro de datos con un tiempo de autonomía suficiente para que se pueda activar el centro de datos alterno
2. Realizar las coordinaciones del caso con el área de Logística para llevar a cabo el mantenimiento periódico del UPS

3. ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades preventivas (antes)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Validar que el UPS este activo y en operación durante el corte de fluido eléctrico.
2. Realizar el apagado de los equipos y/o dispositivos cuyo uso no sea prioritario.
3. Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.

4. ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

	RESPONSABILIDAD			
ACTIVIDADES	GPPI	AST	CTIC	GG
Actividades de recuperación (después)	I	R	AC	I

R: Encargado A: Responsable C: Consultado I: Informado

ASISTENTE DE SOPORTE TÉCNICO (AST)

1. Constatar el buen funcionamiento de todos los equipos y dispositivos de computo.

COORDINADOR DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (CTIC)

1. Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
2. Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.