MINISTERIO
DE AGRICULTURA
Y GANADERIA

GOBIERNO
DE EL SALVADOR

CENTA
Centro Nacional de Tecnología
Agropecuaria y Forestal
Enrique Álvarez Córdova

UNIDAD DE INFORMÁTICA
GERENCIA ADMINISTRATIVA Y FINANCIERA
CENTA

PLAN DE CONTINGENCIA DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

SAN ANDRES

FEBRERO 2019

DIRECTOR
EJECUTIVO

ÍNDICE

CONTENIDO	PÁG.
INTRODUCCIÓN.....	4
II. OBJETIVOS.....	4
III. BASE LEGAL.....	4
IV. FINALIDAD	4
V. ALCANCE.....	5
VI. RESPONSABILIDAD EN LA EJECUCION DEL PLAN	5
VII. DETERMINACIÓN DE RIESGOS	6
VIII. MEDIDAS DE CONTINGENCIA	7
IX. INFRAESTRUCTURA REQUERIDA	16
X. LISTA DE PROCESOS Y RESPONSABLES.....	17
XI. RECURSOS DISPONIBLES Y NO DISPONIBLES PARA CADA PROCESO	19
XII. PROCEDIMIENTOS	21

XIII. VIGENCIA..... 37

XIV. ANEXOS 38

DIRECTOR EJECUTIVO

PLAN DE CONTINGENCIAS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES DEL CENTA

I.- INTRODUCCION

Los Sistemas de Información significan para la Institución un importante avance en materia de modernización de los servicios ofrecidos al público usuario y a las áreas internas de la Institución.

La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y computadoras se hace imprescindible tomar medidas que garanticen una continuidad en la operatividad de estos sistemas, para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempos.

En el Plan de Contingencias se identifican los riesgos a los que están expuestos los sistemas y se precisan las medidas de previsión para minimizarlos, así como los requerimientos inmediatos para atenderlos cuando se produzcan.

II.- OBJETIVOS

Definir y programar la implementación de las medidas de seguridad que garanticen el funcionamiento continuo de los sistemas de información y de comunicaciones del CENTA.

Restaurar los sistemas en forma eficiente con el menor costo y pérdidas posibles, en caso se produzca un incidente se incluyen las medidas de previsión.

III.- BASE LEGAL

a) Normas Técnicas de Control Interno
b) Reglamento de Informática del CENTA
c) Políticas de Gestión Informática del CENTA

IV.- FINALIDAD

Disponer de un plan que permita atender de manera ordenada y prevista situaciones que pongan en riesgo la operatividad de los Sistemas de Información y de comunicaciones en el CENTA, estableciendo procedimientos que eviten interrupciones en su operación.

V.- ALCANCE

La presente Directiva es de observancia y estricto cumplimiento de todo el personal del CENTA, sea cual fuere su régimen laboral.

VI. RESPONSABILIDAD EN LA EJECUCIÓN DEL PLAN

La ejecución del plan de contingencia será responsabilidad de la Unidad de Informática y la Gerencia Administrativa y Financiera del CENTA con el apoyo del comité de contingencia.

Comité de contingencia

El Comité de Contingencia, será el responsable de coordinar las acciones inmediatas para dar una respuesta oportuna dentro de las primeras horas críticas posteriores al inicio de una situación de contingencia.

El Comité de Contingencia está compuesto por:

Ing. Rafael Alemán	Cargo: Director Ejecutivo
Lic. Efraín Fuentes	Cargo: Gerente Administrativo y Financiero
Ing. Manuel Osorio	Cargo: Gerente de Investigación y Desarrollo Tecnológico
Ing. Francisco Torres	Cargo: Gerente de Transferencia Tecnológica y Extensión
Lic. Ana María Rico	Cargo: Jefa Servicios Administrativos
Ing. Ana Luisa Cordero	Cargo: Jefa Unidad de Informática.

Grupo de Apoyo

El grupo de apoyo de contingencia estará formado por todos los técnicos de la Unidad de Informática.

DIRECTOR EJECUTIVO

VII. DETERMINACIÓN DE RIESGOS

Los sistemas mecanizados están expuestos a distintas clases de riesgos, que pueden afectar su normal funcionamiento, por lo que los problemas potenciales se han clasificado en grupos que se detallan a continuación:

Factores Naturales y Artificiales

Son originados por causas externas a la institución y cuyo grado de previsión es muy reducido. Se consideran dentro de este grupo a los factores naturales como temblores, terremotos, maremotos, huracanes entre otros similares; artificiales como incendios, inundaciones, robos y problemas de terrorismo. Estos percances pueden generar pérdidas o daños físicos en las diferentes instalaciones del CENTA (equipos, mobiliario e incluso en personas).

Factores de Servicios

Los riesgos identificados en este grupo pueden generar la interrupción del procesamiento de la información en línea, lo que afectaría seriamente la atención al público; por ejemplo:

a) Caídas en los circuitos dedicados de comunicaciones.
b) Corte de energía eléctrica.

Estos riesgos están asociados con el funcionamiento de los equipos , cuyo deterioro o mal uso puede implicar lo siguiente:

a) Daños en componentes de hardware (discos duros, adaptadores de red, etc.).
b) Fallas en dispositivos de comunicaciones (switches, routers).
c) Desperfectos en las Equipos de Computo é impresoras de las áreas usuarias.
d) Daños graves en los archivos del sistema por errores de hardware o software.
e) Software corrupto o incompatible (copia sin licencia).
f) Virus que dañen los archivos y hasta los equipos.

Factores de Recursos Humanos

Están relacionados con la ausencia o presencia insuficiente de las personas en el mantenimiento de las aplicaciones. Podrían causar demoras en atención de desperfectos; daños en los archivos, equipos y otros dispositivos que requieren personal entrenado para su operación.

Estos riesgos pueden estar motivados por:

a) Administradores no capacitados.

b) Acceso de personas no autorizadas al cuarto de servidores.

VIII.- MEDIDAS DE CONTINGENCIA

A continuación se detallan las medidas que deberán ser aplicadas para minimizar los riesgos de interrupción de los sistemas mecanizados.

Adicionalmente, se menciona los impactos de los riesgos, su probabilidad de ocurrencia, de acuerdo a las cinco categorías siguientes:

a) Muy Alta

b) Alta Mediana

c) Media

d) Baja

e) Muy Baja

Se detallan los riesgos clasificados en las categorías antes especificadas:

Factores Naturales y Artificiales:

Riesgo	**Desastres naturales (terremotos, maremotos, huracanes, etc) y artificiales (incendio, inundación, terrorismo, robo, vandalismo, etc.)**
Probabilidad de Ocurrencia	Mediana
Efecto	• Posible deterioro / inutilización de las instalaciones del CENTA. • En casos muy graves, inutilización total de servidores de aplicación y equipos de comunicación. • Incapacidad temporal para utilizar sistemas mecanizados, servidores y equipos.
Medidas de Previsión	• Entrenamiento del personal para asumir funciones alternas en caso de desastre. • Sistemas de extinción de fuego (extinguidores). • Mobiliario especial (racks) para los equipos críticos (servidores, equipos de comunicaciones). • Mantener contacto con proveedores y/o instituciones que provean equipos de características similares a los del CENTA, con capacidad de alquiler o préstamo en caso de quedar inutilizada totalmente la capacidad operativa. • Retiro o reemplazo de todo tipo de objetos que en caso de incendio puedan ayudar a la expansión del fuego • Revisión continua del estado del cableado de energía eléctrica. • En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura. • Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca de las conexiones eléctricas. • El Cuarto de Servidores, debe contar con una caja principal de corriente. • Prohibición total de fumar en el área sensible. • Contar con vigilancia las 24 horas al día
Acciones de Previsión y Recuperación	• En ese momento cualesquiera sean los procesos que se estén ejecutando se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador". Seguidamente apagar los servidores. • Proveer cubiertas protectoras para cuando el equipo esté apagado. • Se apagara (poner en OFF) la caja principal de corriente del cuarto de servidores. • Si se trata de un incendio de mediana magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local.

Facto res de Servicios

Riesgo	**Corte Prolongado de la Energía Eléctrica**
Probabilidad de Ocurrencia	Mediana
Efecto	• Paralización total de las actividades del CENTA. Servicio restringido, se mantendría la operatividad con equipamiento mínimo.
Medidas de Previsión	• Otorgar mantenimiento preventivo de todo el equipo relacionado.
Acciones de Recuperación	• Poner en funcionamiento una fuente de energía alternativa para la alimentación de equipos del cuarto de servidores. Distribuir la energía eléctrica de acuerdo a lo crítico de su actividad.

Riesgo	**Caidas de Circuitos Integrados**
Probabilidad de Ocurrencia	Mediana
Efecto	Se produciría una paralización de los servicios de telecomunicaciones. • Interrupción del servicio de correo electrónico. • Imposibilidad de acceso a internet.
Medidas de Previsión	• De acuerdo al tipo de equipo contar como mínimo con un equipo de backup para su reemplazo, en caso de que sea necesario. • Contar con un UPS exclusivo para el cuarto de servidores.
Acciones de Recuperación	• Realizar los procedimientos establecidos para verificar si el corte es producido por la empresa de telecomunicaciones o fallas en los equipos de comunicaciones. • Coordinar con la empresa de telecomunicaciones la reposición del servicio o enmendar la falla del equipo de comunicaciones.

Riesgo	**Falta del Servicio de Hosting**
Probabilidad de Ocurrencia	Mediana
Efecto	• Se produciría una paralización de la página Web • Interrupción del servicio de correo electrónico
Medidas de Previsión	• Tener un backup de la estructura y aplicativos alojados en la página web. • Tener backup de las cuentas de correo electrónico
Acciones de Recuperación	• Realizar los procedimientos establecidos para verificar si la falla es producida por la empresa que provee el servicio. • Coordinar con la empresa el restablecimiento del servicio.

Factores de Sistemas

Riesgo	**Falla en Componentes de la Red de Comunicación de Datos**
Probabilidad de Ocurrencia	Mediana
Efecto	• Fallas en switches principales paralizarían la red totalmente, hasta su reemplazo. • Fallas en las controladoras de redes de estaciones de trabajo é impresoras paralizarían el trabajo de la estación de la controladora de red afectada, hasta su reemplazo (hardware).
Medidas de Previsión	• Contar con mantenimiento preventivo para equipos de comunicaciones. Se deberá estar en capacidad de reemplazar temporalmente un dispositivo afectado hasta su reparación. • Mantener un stock mínimo de dispositivos de comunicaciones que garanticen el reemplazo inmediato de los equipos afectados. • Mantenimiento periódico del circuito de toma a tierra • Contar con un UPS exclusivo para los equipos de comunicaciones.

Riesgo	**Desperfectos en Estaciones de Trabajo y/o Impresoras de las Áreas Usuarias**
Probabilidad de Ocurrencia	Mediana
Efecto	Imposibilidad de disponer de información en forma oportuna.
Medidas de Previsión	• Se deberá contar con mantenimiento preventivo y correctivo para los equipos de cómputo (por la misma institución u outsorcing). • Las áreas usuarias deberán respetar estrictamente el calendario de mantenimiento preventivo, lo cual servirá para evaluar el estado de los dispositivos. • Durante el mantenimiento, se recomienda la permanencia del personal de la oficina, para el asesoramiento respectivo.

Riesgo	**Fallas en los Servidores**
Probabilidad de Ocu rrencia	Baja
Efecto	Paralización de atención a usuarios internos y externos, que utilicen las aplicaciones de los servidores.
Medidas de Previsión	• Contar con mantenimiento de hardware y software tanto preventivo como correctivo. • Si se tiene proveedor del servicio de mantenimiento deberá estar en la capacidad de tener un tiempo de respuesta máximo de 1 hora , producida la llamada de reporte de falla • El proveedor deberá tener un tiempo máximo de reparación de 5 horas, en caso de excederse deberá reemplazar el equipo afectado por otro, con las condiciones mínimas para mantener la operatividad. • Los servidores contaran con UPS con una autonomía de 30 minutos, lo que protegerá de fallas producidas por anormalidades en la provisión de energía eléctrica. • Contar con backup para recuperar la información, de ser el caso.

Riesgo	**Restauración de Backups de Servidores**
Probabilidad de Ocu rrencia	Baja
Efecto	Paralización de atención a usuarios internos y externos, que utilicen las aplicaciones de los servidores.
Medidas de Previsión	• Contar con mantenimiento de hardware y software tanto preventivo como correctivo. • Contar con un servidor alterno donde se puedan realizar pruebas de backup. • Si se tiene proveedor de este servicio deberá tener un tiempo máximo de reparación de 5 horas, en caso de excederse deberá reemplazar el equipo afectado por otro, con las condiciones mínimas para mantener la operatividad. • El servidor alterno deberá contar con UPS con una autonomía de 30 minutos, lo que protegerá de fallas producidas por anormalidades en la provisión de energía eléctrica. • Contar con backup para recuperar la información de ser el caso.

Riesgo	**Daños en los Archivos de los Sistemas Mecanizados Producido por Fallas de Hardware**
Probabilidad de Ocurrencia	Mediana
Efecto	La pérdida total o parcial de datos ocasionaría problemas en la atención en línea y en la disponibilidad de la información. Paralización temporal en la atención de usuarios internos y externos.
Medidas de Previsión	• Implementar una política de respaldo de información, teniendo en consideración el volumen de ésta , frecuencia de actualización , frecuencia de consulta , usuarios. • Realizar mantenimiento periódico a los dispositivos para las copias de seguridad, reemplazando las unidades defectuosas. • Almacenar los medios magnéticos de backup en un lugar donde reciban las condiciones mínimas para su conservación. • Contar con almacenamiento externo para copias de seguridad.

Riesgo	**Daños en los Archivos por Virus Informáticos**
Probabilidad de Ocurrencia	Alta
Efecto	• Paralización de los servidores y estaciones de trabajo al atacar el virus al sistema operativo. • Destrucción y alteración de archivos causando paralización temporal de las actividades.
Medidas de Previsión	• Restringir el uso libre de CDs y dispositivos usb , al ser los principales medios de contaminación. • Contar con Software Antivirus, instalando en cada servidor de aplicación y estación de trabajo. • Contar con políticas de actualización continua de Antivirus. • Tener como norma la revisión con Software Antivirus de todos los archivos provenientes desde el exterior del CENTA, vía Cd , dispositivo USB , correo electrónico, internet, etc.

Factores de Recursos Humanos

Riesgo	**Ausencia de Personal**
Probabilidad de Ocurrencia	Mediana
Efecto	• En el caso que el personal encargado del adecuado funcionamiento del sistema no pudiera presentar a laborar, se podría ver afectada la operatividad del mismo y no se daría una adecuada atención a los usuarios. • El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos y otros dispositivos que requieren entrenamiento para su operación.
Medidas de Previsión	• Implementación de manuales de operaciones y procedimientos en los que se detallen claramente todas las labores diarias que se llevan a cabo por cada proceso operativo del sistema. • Aplicación de políticas de rotación para que cada persona esté familiarizada con las distintas labores que se llevan a cabo en cada área.

Medidas de Previsión	• Contar con el número adecuado de personal encargado del funcionamiento del sistema (de tal manera que si una persona no se presenta, las labores no se verían afectadas en alto grado). • El personal a contratarse, así como el personal actual deberá en lo posible tener la disponibilidad para presentarse al CENTA fuera de horario establecido, en caso de ser necesario.

Riesgo	**Falta de Personal**
Probabilidad de Ocurrencia	Mediana
Efecto	• En el caso que el personal que no se tenga un encargado del adecuado funcionamiento de los sistema, se podría ver afectada la operatividad del mismo y no se daría una adecuada atención a los usuarios. • El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos y otros dispositivos que requieren entrenamiento para su operación.
Medidas de Prevision	• Implementación de manuales de operaciones y procedimientos en los que se detallen claramente todas las labores diarias que se llevan a cabo por cada proceso operativo del sistema. • Aplicación de políticas de rotación para que cada persona esté familiarizada con las distintas labores que se llevan a cabo en cada área.
Medidas de Prevision	• Contar con el número adecuado de personal encargado del funcionamiento del sistema (de tal manera que si una persona no se presenta, las labores no se verían afectadas en alto grado). • El personal a contratarse, así como el personal actual deberá en lo posible tener la disponibilidad para presentarse al CENTA fuera de horario establecido, en caso de ser necesario.

Riesgo	**Inadecuada actualización de la Pagina Web**
Probabilidad de Ocurrencia	Alta
Efecto	• Sitio web este fuera de línea • Destrucción y alteración de archivos causando paralización temporal de la publicación del sitio web
Medidas de Prevision	• Contar con manual de usuario de la página web • Contar con políticas de actualización de la página web

Riesgo	**Acceso de Personas No Autorizadas a los Sistemas**
Probabilidad de Ocurrencia	Mediana
Efecto	La manipulación del sistema por personas no autorizadas puede generar graves problemas, desde causar desperfectos en el funcionamiento hasta incluir modificaciones al mismo.
Medidas de Prevision	• Cuando un empleado renuncie o salga de vacaciones, su clave de acceso deberá ser desactivada del sistema para evitar que en su ausencia otra persona pueda acceder al mismo y manipular los dispositivos. • Toda modificación de la estructura de la información en las bases de datos deberá ser autorizada por el jefe de la Unidad de Informática del CENTA. • El uso de passwords personales para la operación de los Sistemas será responsabilidad y uso exclusivo del dueño del password, puesto que cada acceso será grabado en una bitácora de acceso al área de servidores. • Política mensual de expiración de password a usuario. • Todo password deberá tener una longitud mínima de ocho caracteres alfanuméricos. • El acceso al cuarto de servidores del CENTA, debe estar restringido sólo al personal autorizado por la Jefatura de la Unida de Informática del CENTA

IX. INFRAESTRUCTURA REQUERIDA

1) Área para servidores alterna con las características, condiciones ambientales, suministros eléctricos y de seguridad adecuados para los equipos de cómputo y telecomunicaciones.

2) Equipos de cómputo y telecomunicaciones necesarios para su completa y correcta funcionalidad. (servidores, switch, enlaces, router, entre otros.)

3) Área de operación para personal.

4) Facilidades de uso del inmueble (estacionamiento, equipos de oficina, etc.)

X. LISTA DE PROCESOS Y RESPONSABLES

No.	PROCESO	UNIDAD RESPONSABLE	CARGO DEL RESPONSABLE	NOMBRE DEL RESPONSABLE
1	Falla del Servidor de Producción/Desarrollo.	Informática	Jefa de Informática Técnico en Informática	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Angel Artiga
2	Falla de la Base de Datos y/o configuración del Servidor Producción/Desarrollo.	Informática	Jefa de Informática Técnico en Informática	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Angel Artiga
3	Falla en Dispositivos de Comunicación de la Red.	Informática	Jefa de Informática Técnico en Informática	Ing. Ana Luisa Cordero Sr. Dagoberto Mejia.
4	Falla en Cableado estructurado de Red Física y Lógica.	Informática	Jefa de Informática Técnico en Informática	Ing. Ana Luisa Cordero Sr. Dagoberto Mejia.
5	Falla de los UPS. (Equipo)	Informática	Jefa de Informática Técnico en Informática	Ing. Ana Luisa Cordero Sr. Allan González Sr. Fausto Zavala
6	Falta del servicio de internet.	Informática	Jefa de Informática Técnico en Informática	Ing. Ana Luisa Cordero Sr. Alvaro Crespín Sr. Dagoberto Mejia
7	Falla del Servidores por Actualizaciones de Objetos y/o aplicativos de forma errónea.	Informática	Jefa de Informática Técnico en Informática	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Angel Artiga

No.	PROCESO	UNIDAD RESPONSABLE	CARGO DEL RESPONSABLE	NOMBRE DEL RESPONSABLE
8	Falla en Dispositivos de Almacenamiento.	Informática	Jefe de Informática Técnico en Informática	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Angel Artiga Sr. Alvaro Crespín Sr. Dagoberto Mejia Sr. Allan González Sr. Fausto Zavala
9	Fallas en Enlace de Comunicación entre el CENTA y el Ministerio de Hacienda.	Informática	Jefe de Informática Técnico en Informática	Ing. Ana Luisa Cordero Sr. Alvaro Crespín
10	Fallas en los Sistemas de Información instalados generados por Hardware.	Informática	Jefe de Informática Técnico en Informática	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Angel Artiga
11	Fallas en los Sistemas de Información instalados generados por software.	Informática	Jefe de Informática Técnico en Informática	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Angel Artiga
12	Falla en Servicio Hosting.	Informática	Jefe de Informática Técnico en Informática	Ing. Ana Luisa Cordero Sr. Alvaro Crespín.
13	Falla Planta Telefónica.	Informática	Jefe de Informática Técnico en Informática	Ing. Ana Luisa Cordero Sr. José Antonio Huezo

XI.RECURSOS DISPONIBLES Y NO DISPONIBLES PARA CADA PROCESO

No.	PROCESO	RECURSOS DISPONIBLES	RECURSOS NO DISPONIBLES
1	Falla del Servidor de Producción/Desarrollo.	Copias de software. Kit de Herramientas. Stock de Repuestos. Dispositivos de almacenamiento externo. Servidor Virtual	Sitio alterno
2	Falla de la Base de Datos y/o configuración del Servidor Producción/Desarrollo.	Copias de Software. Kit de Herramientas. Stock de Repuestos. Dispositivos de almacenamiento externo. Servidor Virtual	Sitio alterno
3	Falla en Dispositivos de comunicación de Red.	Stock de Repuestos Kit de Herramientas.	
4	Falla en Cableado Estructurado de la Red Física y Lógica.	Bitácoras de Configuración. Kit de Herramientas.	
5	Falla de los UPS (Equipo)	Kit de Herramientas. Stock de UPS	Cantidad suficiente de UPS para cambio
6	Falla del Servicio de Internet	Servicio Telefónico. Expediente del Servicio.	
7	Falla de Servidores por Actualizaciones de Objetos y/o aplicativos de forma errónea.	Copias de Software. Dispositivos de almacenamiento externo. Servidor Virtual	Sitio alterno

No.	PROCESO	RECURSOS DISPONIBLES	RECURSOS NO DISPONIBLES
8	Falla en Dispositivos de Almacenamiento.	Copias de Software. Expediente del Equipo (según caso) Kit de Herramientas. Stock de Repuestos.	
9	Fallas en enlace de comunicación entre el CENTA y el Ministerio de Hacienda.	Servicio Telefónico. Correo electrónico. Expediente del Servicio.	
10	Fallas en los Sistemas de Información instalados generados por Hardware.	Copias de los Sistemas de Información y base de datos. Copias de Software. Kit de Herramientas. Stock de Repuestos. Dispositivos de almacenamiento externo. Servidor Virtual.	Sitio alterno
11	Fallas en los Sistemas de Información instalados generados por software.	Copias de los Sistemas de Información y base de datos. Copias de Software. Dispositivos de almacenamiento externo. Servidor Virtual.	Sitio alterno
12	Falla en servicio de Hosting	Servicio Telefónico. Correo electrónico. Expediente del Servicio	
13	Falla en planta Telefónica	Servicio Telefónico. Expediente del Servicio	

1. PROCEDIMIENTO A SEGUIR EN FALLA DEL SERVIDOR DE PRODUCCIÓN / DESARROLLO

Tiempo Máximo Global de Contingencia: 24 Horas

NO.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Se verifica el tipo de falla Si la Falla es de Hardware y se puede solventar internamente se realiza el procedimiento siguiente: ➢ Se repara o sustituye la parte con el Stock de Repuestos existente. ➢ Se verifica la Configuración del servidor para la Puesta en Operación. (Si se ha realizado un reinicio de Sistema Operativo a causa de la sustitución del hardware ya se parcial o total se restauran los respaldos correspondientes). ➢ Puesta en Operación del Servidor Si la falla es de software y se puede solventar internamente se realiza el procedimiento siguiente: ➢ Se repara, instala o desinstala el software según el caso ➢ Se verifica la Configuración del servidor para la puesta en Operación. ➢ Si se ha realizado un reinicio de Sistema Operativo, se restauran los respaldos correspondientes. ➢ Puesta en marcha del servidor.	Ing. Néstor Fabián Sr. Angel Artiga
2	Si la Falla no se puede solventar internamente se realiza lo siguiente: ➢ Se comunica inmediatamente con un Proveedor del Servicio de reparación o mantenimiento de servidores y/o equipo, que pueda proporcionar la asesoría y/o repuesto necesario y adecuado para resolver el problema. ➢ Si el equipo posee garantía, se debe de gestionar ante el proveedor o fabricante. Para que se sustituya o repare el equipo y/o servidor. Si existiere una cláusula de continuidad de negocio en marcha, el proveedor local, deberá de proporcionar un equipo en calidad de préstamo, mientras se repara o sustituye el equipo.	Ing. Ana Luisa Cordero Ing. Néstor Fabián Colocho Sr. Angel Artiga

2. PROCEDIMIENTO A SEGUIR EN FALLA DE LA BASE DE DATOS Y/O CONFIGURACIÓN DE SERVIDORES

Tiempo Máximo Global de Contingencia: 24 Horas.

NO.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
	Se verifica el tipo de falla Si la Falla es de Software y se puede solventar internamente se realiza el procedimiento siguiente: ➢ Se verifica la Configuración del servidor y/o equipo para la Puesta en Operación. (Si es necesario se debe de restaurar el respaldo correspondiente). ➢ Se deberá de Restaurar todas las configuraciones, desinstalar último software, actualizar cada uno de los controladores de hardware o de componentes del servidor, ya sean estos FrameWorks, motores de bases de datos, Motores de Servidores Web, Core y políticas de acceso a directorios, ➢ Puesta en Operación del Servidor de Producción/Desarrollo y/o Equipo. Si la falla es de Hardware y se puede solventar internamente se realiza el procedimiento siguiente: ➢ Se verifica la Configuración del servidor y/o equipo para la Puesta en Operación. (Si es necesario se debe de restaurar el respaldo correspondiente). ➢ Se deberá de Restaurar todas las configuraciones, desinstalar último hardware conectado al equipo y/o actualizar los controladores del mismo. ➢ Puesta en Operación del Servidor de Producción/Desarrollo y/o Equipo.	Ing. Néstor Fabián Sr. Angel Artiga

	Se verifica el tipo de falla Si la Falla es de Software y se puede solventar internamente se realiza el procedimiento siguiente: ➢ Se verifica la Configuración del servidor y/o equipo para la Puesta en Operación. (Si es necesario se debe de restaurar el respaldo correspondiente). ➢ Se deberá de Restaurar todas las configuraciones, desinstalar último software, actualizar cada uno de los controladores de hardware o de componentes del servidor, ya sean estos FrameWorks, motores de bases de datos, Motores de Servidores Web, Core y políticas de acceso a directorios, ➢ Puesta en Operación del Servidor de Producción/Desarrollo y/o Equipo. Si la falla es de Hardware y se puede solventar internamente se realiza el procedimiento siguiente: ➢ Se verifica la Configuración del servidor y/o equipo para la Puesta en Operación. (Si es necesario se debe de restaurar el respaldo correspondiente). ➢ Se deberá de Restaurar todas las configuraciones, desinstalar último hardware conectado al equipo y/o actualizar los controladores del mismo. ➢ Puesta en Operación del Servidor de Producción/Desarrollo y/o Equipo.	Ing. Néstor Iván Fabián Colocho Sr. Angel Artiga

3. PROCEDIMIENTO A SEGUIR EN FALLA EN DISPOSITIVOS DE COMUNICACIÓN DE RED

Tiempo Máximo Global de Contingencia: 5 Horas.

NO.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Si la Falla del Hardware se puede solventar internamente se realiza el procedimiento correspondiente. ➢ Se sustituye ô se repara la parte con el Stock de repuestos existentes. ➢ Se verifica la Configuración del Equipo para la Puesta en operación ➢ Puesta en Operación del Equipo (Switches/router/AP).	Sr. Dagoberto Mejía Sr. Allan Gonzalez Sr. Fausto Zavala
2	Si la Falla del Hardware es seria y no se puede solventar internamente se realiza lo siguiente: ➢ Se comunica inmediatamente con el proveedor de los dispositivos para hacer efectiva la garantía o Cláusula de Préstamo de Equipo, mientras el proveedor resuelve el problema ➢ Si el equipo no tiene garantía, se debe realizar requerimiento de compra.	Ing. Ana Luisa Cordero Sr. Dagoberto Mejía

4. PROCEDIMIENTO A SEGUIR FALLA EN CABLEADO ESTRUCTURADO DE LA RED FÍSICA Y LÓGICA

Tiempo Máximo Global de Contingencia: 8 Horas.

NO.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Si la Falla se puede solventar internamente se realiza el procedimiento correspondiente. ➢ Se verifica conexión en punto de Red para determinar la falla. ➢ Se sustituye ô se repara la parte con el Stock de Repuestos existente ➢ Conexión y puesta en operación del Punto de Red.	Sr. Dagoberto Mejía, Sr. Fausto Zavala Sr. Allan González
2	Si la Falla es seria y No se puede solventar internamente se realiza lo siguiente: ➢ Se elabora requerimiento para contratación del servicio o compra de insumos para resolver el problema.	Ing. Ana Luisa Cordero Sr. Dagoberto Mejía

5. PROCEDIMIENTO A SEGUIR EN FALLA DE LOS UPS (EQUIPO)

Tiempo Máximo Global de Contingencia: 8 Horas.

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Si la Falla del Equipo se puede solventar internamente se realiza el procedimiento correspondiente. ➢ Se sustituye ô se repara la parte con el Stock de repuestos ➢ Se verifica el Equipo para la puesta en operación. ➢ Puesta en Operación del Equipo (UPS).	Sr. Fausto Zavala y Sr. Allan González.
2	Si la Falla es seria y No se puede solventar internamente se realiza lo siguiente: ➢ Se elabora requerimiento para contratación del servicio requerido para resolver el problema del UPS o compra.	Ing. Ana Luisa Cordero

6. PROCEDIMIENTO A SEGUIR EN FALLA DEL SERVICIO DE INTERNET

Tiempo Máximo Global de Contingencia: 3 Hrs.

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Se verifica que el Servicio de Internet está suspendido o proporcione tiempos de respuesta muy lentos	Sr. Alvaro Crespín Sr. Dagoberto Mejía
2	Se comunica con el Proveedor del Servicio para Informar sobre los problemas existentes, para su pronta solución.	Sr. Alvaro Crespín Sr. Dagoberto Mejía
3	Se monitorea el Servicio de Internet, hasta que se normalice el Servicio.	Sr. Alvaro Crespín Sr. Dagoberto Mejía
4	Se comunica a los Usuarios que el Servicio de Internet ha sido restablecido.	Sr. Alvaro Crespín Sr. Dagoberto Mejía

7. PROCEDIMIENTO A SEGUIR EN FALLA DE SERVIDORES POR ACTUALIZACIONES DE OBJETOS y/o APLICATIVOS DE FORMA ERRÓNEA

Tiempo Máximo Global de Contingencia: 5 Horas.

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Se verifica la Configuración del servidor para la Puesta en Operación.	Ing. Néstor Fabián Sr. Angel Artiga
2	Se recompilan o se restaura el Back up correspondiente.	
3	Se realizan los cambios correspondientes y apropiados en los objetos o aplicativo.	
4	Puesta en Operación del Servidor de producción/Desarrollo.	

8. PROCEDIMIENTO A SEGUIR EN FALLA EN DISPOSITIVOS DE ALMACENAMIENTO

Tiempo Máximo Global de Contingencia: 8 Horas.

NO.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Si la Falla del dispositivo de almacenamiento se puede solventar internamente se realiza el procedimiento siguiente: ➢ Se verifica que el dispositivo no se encuentre dañado de forma física o lógica. ➢ Si la falla que presenta es lógica, se realiza la actualización de controladores y del servidor, y que son los intérpretes entre el hardware y el software o se sustituyen. ➢ Si la falla es de hardware se sustituye y se verifica la Configuración del equipo para su buen funcionamiento. ➢ Se pone en Operación el Dispositivo.	Ing. Néstor Fabián Sr. Alvaro Crespin Sr. Allan Gonzalez, Sr. Fausto Zavala Sr. Angel Artiga Sr. Dagoberto Mejia
2	Si la Falla en el dispositivo no se puede solventar internamente se realiza lo siguiente: ➢ Se comunica inmediatamente con el proveedor del equipo, para hacer efectiva la garantía cuando esta aplique. ➢ Si el equipo no posee garantía se debe gestionar la compra de un nuevo.	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Alvaro Crespin Sr. Allan Gonzalez, Sr. Fausto Zavala Sr. Angel Artiga Sr. Dagoberto Mejia

9. PROCEDIMIENTO A SEGUIR EN FALLA EN ENLACE DE COMUNICACIÓN ENTRE EL CENTA Y EL MINISTERIO DE HACIENDA

Tiempo Máximo Global de Contingencia: 3 Hrs.

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Se verifica funcionamiento del servicio de Comunicación entre el enlace del CENTA y Ministerio de Hacienda .	Sr. Alvaro Crespín
2	Se comunica con el Proveedor del Servicio para Informar sobre los problemas existentes, para su pronta solución.	Sr. Alvaro Crespín
3	Se comunica con personal del Ministerio de Hacienda para informar los problemas existentes.	Sr. Alvaro Crespín
4	Se monitorea el Servicio, hasta que se normalice.	Sr. Alvaro Crespín
5	Se comunica a los Usuarios que el Servicio de Comunicación entre CENTA y Ministerio de Hacienda ha sido restablecido	Sr. Alvaro Crespín

10. PROCEDIMIENTO A SEGUIR EN FALLAS EN LOS SISTEMAS DE INFORMACIÓN INSTALADOS GENERADAS POR HARDWARE

Tiempo Máximo Global de Contingencia: 5 Horas.

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Si la Falla del Hardware se puede solventar internamente se realiza el Procedimiento correspondiente. ➢ Se verifica que hardware está creando la falla en los sistemas ➢ Se sustituye o repara el hardware que genera la falla. ➢ Se verifica la configuración del equipo y/o servidor para la puesta en operación. ➢ Si la falla genero un restablecimiento de configuración o reinicio de fábrica, se deben de restaurar todos sus componentes de configuración y/o datos a través de una copia de seguridad. ➢ Puesta en Operación del Equipo y/o servidor correspondiente.	Ing. Néstor Fabián Sr. Angel Artiga
2	Si la Falla del Hardware no se puede solventar internamente se realiza lo siguiente: ➢ Se comunica inmediatamente con un Proveedor del Servicio de reparación o mantenimiento de servidores y/o equipo, que pueda proporcionar la asesoría y/o repuesto necesario y adecuado para resolver el problema. ➢ Si el equipo posee garantía, se debe de gestionar ante el proveedor o fabricante. Para que se sustituya o repare el equipo y/o servidor. Si existiere una cláusula de continuidad de negocio en marcha, el proveedor local, deberá de proporcionar un equipo en calidad de préstamo, mientras se repara o sustituye el equipo. ➢ Si la falla genero un restablecimiento de configuración o reinicio de fábrica del equipo, se deben de restaurar todos sus componentes de configuración y/o base de dato a través de una copia de seguridad.	Ing. Ana Luisa Cordero Ing. Néstor Fabián Sr. Angel Artiga

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
	➢ Cuando el Sistema de Información se encuentra instalado en una Computadora Personal, mientras se espera la solución del problema, se realiza el proceso de Instalación y configuración de otro Equipo para el uso del Sistema de Información correspondiente.	

11. PROCEDIMIENTO A SEGUIR EN FALLAS EN LOS SISTEMAS DE INFORMACIÓN INSTALADOS GENERADAS POR SOFTWARE

Tiempo Máximo Global de Contingencia: 5 Horas.

No.	ACTIVIDADES QUE SE REALIZAN	Responsable Operativo
1	Si la Falla del Software se puede solventar internamente se realiza el Procedimiento correspondiente: ➢ Se verifica la Configuración del Equipo y/o Servidor para su Puesta en Operación y catalogar las incompatibilidades de las aplicaciones con los nuevos softwares, llámese estos sistemas operativos, antivirus, motores de base de datos, librerías de ejecución y cualquier otro componente que permita generar una falla. ➢ Se deberá de desinstalar último software, actualizar cada uno de los controladores de hardware o de componentes del servidor, ya sean estos FrameWorks, motores de bases de datos, Motores de Servidores Web, Core y políticas de acceso a directorios, ➢ Puestaen Operación del Equipo y/o Servidor correspondiente. ➢ Si se reestableció el reinicio de fábrica, se deberá de instalar las diferentes Licencias de Software y Sistemas de Información que se encontraban inicialmente, incluyendo sus bases de datos. ➢ Se verifica el buen funcionamiento de los Sistemas de Información instalados como su base de datos. ➢ Puesta en Operación de los Sistemas de Información.	Ing. Néstor Fabián Sr. Angel Artiga
2	Si la Falla del Software no se puede solventar internamente se realiza lo siguiente: ➢ Se comunica inmediatamente con el Proveedor de Servicios, software y/o Equipo, que pueda proporcionar la asesoría adecuada para resolver el problema o falla.	Ing. Néstor Fabián Sr. Angel Artiga

No.	ACTIVIDADES QUE SE REALIZAN	Responsable Operativo
	➢ Si la falla es por incompatibilidad, se deberá de parchar los softwares que generan esta falla y actualizar los aplicativos. ➢ Si la falla es por obsolescencia de software (desatendido) se deberá de tener una copia de respaldo del mismo, con la documentación necesaria para su uso y posterior instalación. ➢ Cuando el Sistema de Información se encuentra instalado de forma local en una Computadora de Escritorio o Portátil, se realiza el proceso de Instalación y configuración de otro Equipo para el uso del Sistema de Información correspondiente, mientras se espera la solución del problema.	

12. PROCEDIMIENTO A SEGUIR EN FALLA EN SERVICIO DE HOSTING

Tiempo Máximo Global de Contingencia: 4 Hrs.

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Se verifica funcionamiento del Servicio de correo, pagina web y aplicaciones web	Sr. Alvaro Crespín
2	Se comunica con el Proveedor del Servicio para Informar sobre los problemas existentes, para su pronta solución.	Sr. Alvaro Crespín
3	Se monitorea el Servicio, hasta que se normalice.	Sr. Alvaro Crespín.
4	Se comunica a los Usuarios que el Servicio de correo y pagina web y aplicaciones web ha sido restablecido.	Sr. Alvaro Crespín

13. PROCEDIMIENTO A SEGUIR EN FALLA EN PLANTA TELEFÓNICA

Tiempo Máximo Global de Contingencia: 5 Hrs.

No.	ACTIVIDADES QUE SE REALIZAN	RESPONSABLE OPERATIVO (NOMBRE/CARGO)
1	Se verifica funcionamiento del Servicio.	Sr. Jose Antonio Huezo
2	Se comunica con el Proveedor del Servicio para Informar sobre los problemas existentes, para su pronta solución.	Sr. Jose Antonio Huezo
3	Se comunica con el Proveedor del E1 para Informar sobre los problemas existentes, para su pronta solución.	Sr. Jose Antonio Huezo
4	Se monitorea el Servicio, hasta que se normalice.	Sr. Jose Antonio Huezo.
5	Se comunica a los Usuarios que el Servicio ha sido restablecido.	Sr. Jose Antonio Huezo

XIII. VIGENCIA

Su temporalidad es permanente y podrá ser modificado al identificarse nuevas áreas de riesgo que pudieran generar contingencia.

Aprobado a los cuatro días del mes de febrero del año dos mil diecinueve en la Dirección Ejecutiva del Centro Nacional de Tecnología Agropecuaria y Forestal "Enrique Álvarez Córdova".

Aprobado:

Ing. Rafael Antonio Alemán
Director Ejecutivo

XIV. ANEXOS

1. LISTA DE TELEFONOS DE EMERGENCIA
2. FICHAS DE RESPONSABLES DE LOS PROCESOS

LISTA DE TELEFONOS DE EMERGENCIA

Servicio	Teléfono
A. Línea de Emergencia	911
B. Servicios Médicos ISSS Santa Tecla	2597-2170
C. Ambulancias Cruz Roja Salvadoreña	2222-5155
D. Cuerpo de Bomberos Antiguo Cuscatlán Cuartel central	2243-2054 913
E. Policía Nacional Civil PNC- Ciudad Arce	2330-9322
F. Ministerio de Hacienda	2244-3444
G. Ministerio de Agricultura y Ganadería	2210-1700

FICHA
RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Ing. Ana Luisa Cordero.**

Proceso

1. **Falla del Servidor de Producción/Desarrollo.**
2. **Falla de la base de datos y/o configuración del servidor de Producción/Desarrollo.**
3. **Falla en Dispositivos de comunicación de Red.**
4. **Falla en cableado estructurado de la red física y lógica**
5. **Falla de los UPS (Equipo).**
6. **Falla en el servicio de internet**
7. **Falla del Servidor de Producción/Desarrollo por actualizaciones de Objetos y/o Aplicativos de forma errónea.**
8. **Falla en Dispositivos de Almacenamiento**
9. **Falla en enlace de comunicación entre el CENTA y Ministerio de Hacienda**
10. **Fallas en los Sistemas de Información instalados, generados por el Hardware.**
11. **Fallas en los Sistemas de Información instalados generados por el Software.**
12. **Falla en servicio de Hosting.**
13. **Falla en Planta Telefónica.**

ÁREA : Unidad de Informática.

CARGO : Jefa Unidad de Informática.

DIRECCIÓN : Res. Scorpio senda 14 No. 43 Ciudad Corinto, Mejicanos.

TELÉFONO OFICINA : 2397-2287, Ext. 287.

TELÉFONO CELULAR : 79196450.

OBSERVACIONES:

FICHA RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Ing. Néstor Fabián Colocho**

Proceso	**1**	**Falla del Servidor de Producción/Desarrollo.**
	2	**Falla de la base de datos y/o configuración del Servidor de Producción/Desarrollo.**
	7	**Falla del Servidor de Producción/Desarrollo por actualizaciones de Objetos y/o Aplicativos de forma errónea.**
	8	**Falla en Dispositivos de Almacenamiento.**
	10	**Fallas en los Sistemas de Información instalados, generados por el Hardware.**
	11	**Fallas en los Sistemas de Información instalados generados por el Software.**

ÁREA : Unidad de Informática.

CARGO : Desarrollador de Aplicaciones

DIRECCIÓN : Cantón San Andrés, lote 3, polígono "A", Casa #1 Ciudad Arce, La libertad,

TELÉFONO OFICINA : 2397-2292, Ext. 292.

TELÉFONO CELULAR : 6131-9945.

OBSERVACIONES:

FICHA
RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Sr. Ángel Artiga.**

PROCESO

1	**Falla del Servidor de Producción/Desarrollo.**
2	**Falla de la base de datos y/o configuración del Servidor de Producción/Desarrollo.**
7	**Falla del Servidor de Producción/Desarrollo por actualizaciones de Objetos y/o Aplicativos de forma errónea.**
8	**Falla en Dispositivos de Almacenamiento.**
10	**Fallas en los Sistemas de Información instalados, generados por el Hardware.**
11	**Fallas en los Sistemas de Información instalados generados por el Software.**

ÁREA : Unidad de Informática.

CARGO : Desarrollador de Aplicaciones.

DIRECCIÓN : Col. Amatepec pasaje 1 Casa #30,
Soyapango, San Salvador.

TELÉFONO OFICINA : 2397-2292, Ext. 292.

TELÉFONO CELULAR : 7819-5474

OBSERVACIONES

FICHA
RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Sr. Álvaro Agustín Crespín Girón**

Proceso

6	**Falla en el servicio de internet**
8	**Falla en Dispositivos de Almacenamiento**
9	**Falla en enlace de comunicación entre el CENTA y Ministerio de Hacienda.**
12	**Falla en servicio de Hosting**

ÁREA	: Unidad de Informática.
CARGO	**:** Administrador de Sistemas y Contenido
DIRECCIÓN	**:** Col. Sitio del Niño, 3a.Calle, Casa No. 10 San Juan Opico, La Libertad.
TELÉFONO OFICINA	**:** 2397-2280, Ext. 280.
TELÉFONO CELULAR	: 7026-9442

OBSERVACIONES:

FICHA
RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Sr. Dagoberto Mejía.**

PROCESO

3	**Falla en Dispositivos de comunicación de Red.**
4	**Falla en cableado estructurado de la red física y lógica.**
8	**Falla en Dispositivos de Almacenamiento.**

ÁREA : Unidad de Informática.

CARGO : Administrador de Red

DIRECCIÓN : Ciudad Versalles, Villa Burdeos, polígono 12 casa #36

TELÉFONO OFICINA : 2397-2280, Ext. 280.

TELÉFONO CELULAR : 71617542

OBSERVACIONES:

FICHA
RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Sr. Allan González.**

PROCESO

4	**Falla en el cableado estructurado de la red física y lógica.**
5	**Falla de los UPS (Equipo).**
8	**Falla en Dispositivos de Almacenamiento.**

ÁREA : Unidad de Informática.

CARGO : Soporte Técnico.

DIRECCIÓN : Col. AltaVista Pol 31 Avenida las Delicias Norte Casa 154, Ilopango.

TELÉFONO OFICINA : 2397-2276, Ext. 276.

TELÉFONO CELULAR : 7140-4233

OBSERVACIONES:

FICHA
RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Sr. Fausto Zavala.**

PROCESO

4	**Falla en el cableado estructurado de la red física y lógica.**
5	**Falla de los UPS (Equipo).**
8	**Falla en Dispositivos de Almacenamiento.**

ÁREA : Unidad de Informática.

CARGO : Soporte Técnico.

DIRECCIÓN : Santa Tecla Nuevo amanecer pasaje 4, No.1140, La Libertad

TELÉFONO OFICINA : 2397-2276, Ext. 276.

TELÉFONO CELULAR : 7386-5982

OBSERVACIONES:

FICHA
RESPONSABLE DEL PROCESO

NOMBRE / RESPONSABLE **Sr. José Antonio Huezo.**

PROCESO

13 **Falla en Planta Telefónica.**

ÁREA : Unidad de Informática.

CARGO : Técnico en Telecomunicaciones.

DIRECCIÓN : Reparto San Fernando pasaje 6 polígono F, Casa No. 20, Soyapango

TELÉFONO OFICINA : 2397-2296, Ext. 296.

TELÉFONO CELULAR :

OBSERVACIONES: