INSTITUTO NACIONAL DE LAS MUJERES | GOBIERNO DE COSTA RICA

CIRCULAR
INAMU-PE-009-2024
PRESIDENCIA EJECUTIVA

ASUNTO:	Divulgación del Plan de Recuperación ante Desastres en Tecnologías de Información.
DE:	Adilia Caravaca Zúñiga, Presidenta Ejecutiva
PARA:	Dirección Estratégica Dirección Administrativa Financiera. Coordinadoras y Coordinadores de Área. Personal encargado de administrar u operar Sistemas de información y telecomunicaciones
FECHA:	19 de junio 2024

Que, con base en la normativa vigente y mejores prácticas en temas de recuperación de ante desastre de tecnologías de información, se emite el siguiente comunicado institucional:

CONSIDERACIONES GENERALES Y MARCO NORMATIVO

Considerando que:

1. El país ha venido asumiendo el reto de incorporarse a la denominada cuarta revolución industrial y las sociedades del conocimiento. Industria 4.0 basada en sistemas ciber-físicos que transformaran los procesos productivos y la calidad de vida de las personas.

2. El actual gobierno, a través de la Estrategia de Transformación Digital 2022-2026, ha establecido una serie de recomendaciones para los ámbitos del Sector Público, Sector Privado y la Academia, con el fin de hacer efectivo el avance en la digitalización en el periodo abarcado entre 2022 y 2026. La visión de la Estrategia es acelerar la productividad y competitividad buscando el desarrollo socioeconómico inclusivo y sostenible, a partir del impulso de transformaciones digitales en la ciudadanía, las empresas, y las entidades públicas, con el fin de asegurar la reconversión empresarial necesaria para la industria 4.0, y mejorar la relación gobierno-ciudadanía.

3. Para cumplir con esta estrategia se ha aprobado una serie de normativa que marca el norte del desarrollo de Tecnologías de información, sobre todo para el sector público, entre las que destacan:

    3.1. Que mediante esta misma Resolución R-DC-17-2020, la CGR, modifica las Normas de Control Interno para el Sector Público (N-2-2009CO-DFOE), los ítems 5.9 y 5.10, para que se lean de la siguiente manera:

- 5.9 Tecnologías de información: El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información. En esa línea, de conformidad con el perfil tecnológico de la institución, órgano o ente, en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica, el jerarca deberá aprobar el marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes. Para la determinación del perfil tecnológico institucional se podrán considerar variables como las siguientes: marco de procesos para la gestión de TI, mapeo de procesos y subprocesos de negocio, organigrama de la entidad, conformación del Comité de TI, proveedores de TI, servicios de TI, inventario y criticidad de tipos documentales, centros de procesamiento y almacenamiento de datos, inventario de equipos y sistemas de información que soportan los servicios, software, proyectos de TI, planes de adquisición sobre TI, canales electrónicos y riesgos de TI.

- 5.10 Sistemas de información y tecnologías de información en instituciones de menor tamaño: El jerarca y los titulares subordinados de las instituciones de menor tamaño, según sus competencias, deben establecer los procedimientos manuales, automatizados o ambos, necesarios para obtener, procesar, controlar, almacenar y comunicar la información sobre la gestión institucional y otra relevante para la consecución de los objetivos institucionales. Dicha información debe ser de fácil acceso y estar disponible en un archivo institucional que, de manera ordenada y conforme a las regulaciones que en esa materia establece el Sistema Nacional de Archivos, pueda ser consultado por usuarios internos o por parte de instancias externas. De igual forma, dichos sujetos, de acuerdo con sus competencias y su perfil tecnológico, definido en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica, deberán aprobar su marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes. (El subrayado no es parte del original).

3.2. Que la CGR establece en su transitorio I de esta misma Resolución R-DC-17-2020, que todas las instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República deberán haber declarado, aprobado y divulgado el marco de gestión de las tecnologías de información y comunicación (el

subrayado no es parte del original) requerido en la modificación incorporada en esta resolución a las Normas de Control Interno para el Sector Público (N-2-2009-CODFOE), a más tardar el 1° de enero del 2022.

4. **Código de Tecnologías Digitales del MICIIT:** Según el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) (2021), este documento constituye un "compendio de políticas públicas que establecen los mínimos deseables para la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en el sector público costarricense" (p. 6).

4.1. Declaración

Todos los temas o principios del código son de aplicación para el plan de TI:

- Accesibilidad, Usabilidad y Experiencia de personas usuarias.
- Identificación y Autentificación Ciudadana.
- Seguridad Tecnológica.
- Infraestructura y Tecnología en la Nube.
- Interoperabilidad.
- Neutralidad Tecnológica.

4.2. Implicación

El documento brinda los criterios técnicos básicos que toda institución pública debe considerar cuando desarrolla iniciativas estratégicas y proyectos digitales. Asimismo, los controles derivados de los aspectos técnicos mencionados en el código de tecnologías digitales impactarán las distintas capas de la arquitectura de información, datos, aplicaciones e infraestructura de la institución; así como procesos de soporte como lo son gestión de la seguridad de la información, continuidad de las operaciones y gestión de ciberseguridad.

5. Que la Junta Directiva del INAMU, aprobó en la Sesión Ordinaria N° 10-2024 celebrada el 08 de abril del 2024, mediante el acuerdo número 3 que indica: "*Se da por recibido y aprobado el documento referente al Plan de Recuperación ante Desastres en Tecnologías de Información, el cual fue previamente aprobado por el Comité Institucional de Tecnologías de Información.*"

Por tanto; con base en las consideraciones anteriores, la Unidad de Informática en cumplimiento de sus competencias, presenta el Plan de Recuperación ante Desastres del INAMU (DRP).

PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP)

El INAMU es una institución pública que soporta sus procesos institucionales, tanto estratégicos como operativos, a través de servicios de tecnologías de información, esto significa que una interrupción o fallos en los componentes tecnológicos podría afectar la operación normal de la Institución, y, por ende, faltar al cumplimiento de su razón de ser. Desde esta perspectiva, la Unidad de Informática ha

diseñado el presente plan de recuperación ante desastres con la intención de definir claramente las pautas a seguir en caso de un eventual desastre tecnológico en la Institución.

Para elaborar este documento se realizaron talleres con las diferentes dependencias del INAMU, desde el año 2018, en el proceso se realizaron labores de sensibilización y concientización en materia de continuidad de servicios de TI y del negocio entre la Unidad de Informática y la Unidad de Planificación, los cuales permitieron identificar los componentes críticos que soportan los procesos institucionales, esta información es base para el desarrollo del presente plan de recuperación.

OBJETIVO

Mantener la continuidad de todos los servicios de Tecnología de la información, a través de un plan de recuperación de la plataforma tecnológica, de forma tal que la institución pueda prestar los servicios a la población usuaria de una manera adecuada, veraz y oportuna mediante el uso de los equipos, servidores y dispositivos tecnológicos.

SERVICIOS CRÍTICOS

Los siguientes servicios se consideran como servicios críticos clasificados con el mayor puntaje, conforme con encuesta realizada al personal del INAMU en el año 2020. El resto de los servicios serán tratado mediante la metodología de trabajo de atención de la mesa de soporte técnico:

1. Protección de los derechos de las mujeres
2. Desarrollo empresarial de las mujeres
3. Gestión Financiera Contable
4. Consulta web institucional
5. Gestión de las capacitaciones
6. Correo Electrónico

ESCENARIO TOTAL O PARCIAL DE DESASTRES

Los escenarios de desastres pueden afectar de manera total o parcial la tecnología de información, en el caso del INAMU se tomará como escenario de desastre total la no disponibilidad del centro de cómputo en su totalidad y como un escenario de desastre parcial, la no disponibilidad de ciertos componentes o dispositivos, necesarios, para el funcionamiento alguno de los 6 servicios más críticos,

los cuales, si fallan pueden impactar la operación de los servicios y por consiguiente la afectación de los procesos de institucionales.

Los escenarios de desastre, interrupción mayor o un evento contingente que contempla este documento guía son:

CENTRO DE CÓMPUTO

El Centro de Cómputo, está compuesto por un conjunto de servidores equipados con el hardware y software necesarios para cumplir esta tarea y conectados a la red institucional de comunicaciones.

Algunas de las razones por las cuales no se pueda disponer del Centro de Datos son las siguientes:

- Incendio
- Inundación
- Daño sistema aire acondicionado
- Daño en suministro eléctrico
- Atentado terrorista

INFRAESTRUCTURA DE COMUNICACIONES

La infraestructura de redes y comunicaciones corresponde a un conjunto de dispositivos, conexiones y enlaces de comunicación, que se utilizan para permitir la comunicación remota entre personas, equipos, dispositivos y departamentos independientes.

La falla en alguno o varios de los dispositivos existentes en la red de comunicaciones, servidores o equipos, sería considerada un desastre, por lo que todos y cada uno de los mismos, deben estar en funcionamiento continuo.

INFRAESTRUCTURA DE BASES DE DATOS, ALMACENAMIENTO Y RESPALDO

Es considerado todo sistema que cuenta con una base de datos, donde se almacenan los datos, o información para lo cual fue elaborado. La administración de bases de datos se realiza mediante un paquete de software que ayuda a administrar las bases de datos de manera segura y efectiva, lo que permite organizar los datos correctamente. La no disponibilidad de datos e información impediría que se puedan utilizar los sistemas, algunas de las fallas que se deben considerar son:

- Corrupción de la base de datos
- Borrado o pérdida de datos
- Falla total o parcial de la red de almacenamiento institucional
- Falla total o parcial del servidor de respaldo

INFRAESTRUCTURA ELÉCTRICA

La infraestructura eléctrica es esencial para el funcionamiento eficiente y confiable de todos y cada uno de los equipos y dispositivos hospedados en el centro de datos, por lo que todos deben estar en

funcionamiento y deben considerarse fuentes alternas que permitan el servicio eléctrico continuo. Algunos de los aspectos que pueden minimizar esta continuidad son:

- Fallos en las fuentes de poder del Centro de Datos
- Planta de energía del Edificio Sigma
- Apagado inesperado de los equipos de respaldo del Centro de Datos.
- Problemas con el transformador

INFRAESTRUCTURA DE ENFRIAMIENTO O DE CLIMATIZACIÓN

Dada la potencia de los equipos y dispositivos del Centro de Datos, es indispensable un equipo de enfriamiento o climatización que permita mantener a bajas temperaturas a todos y cada uno de sus componentes. Por lo que la principal causa de falla es la siguiente:

- Fallos en aires acondicionados primarios instalados.
- Fallos en los servicios de aire acondicionado auxiliares.

ROLES Y RESPONSABILIDADES

Los roles y responsabilidades definidos en este plan deberán ser ejercidos por el personal seleccionado, de forma tal que se minimice el impacto y se actúe de forma adecuada.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
Líder del DRP	Velar por la actualización del DRP y recursos requeridos. - Velar por la actualización, distribución y pruebas del DRP - Gestionar la consecución de los recursos para el DRP. - Comunicar a las personas que corresponda sobre la situación de contingencia.	- Evaluar y activar el DRP y las estrategias de recuperación y contingencia. - Comunicar a la Dirección sobre el estado de la operación de Contingencia. - Informar el momento en que opera en contingencia y que puede suceder con la prestación del Servicio - Liderar la operación bajo contingencia. - Comunicar a la dirección el desastre, interrupción o evento contingente. - Liderar el retorno a la normalidad.	- Velar por la actualización del DRP acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción. - Informar al Dirección sobre el retorno a la normalidad y agradecer la comprensión y apoyo de todos en esta situación.
Líder de infraestructura, Líder de Redes y Comunicaciones, y Líder de Mesa de ayuda (Soporte Técnico)	- Comunicar necesidades de ajuste - Participar en la ejecución de las pruebas al DRP	- Evaluar el desastre, interrupción o evento contingente. - En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución. - Comunicar el evento al Líder del DRP - Verificar disponibilidad y notificar al personal requerido para atender el evento. - Ejecutar las guías de contingencia y recuperación. - Comunicar a los proveedores la activación del DRP. - Solicitar la corrección del componente afectado y realizar seguimiento de la solución. - Estar atentos para dar una correcta información a las personas que lo requieran. - Mantener informado al Líder del DRP	- Reportar los inconvenientes y oportunidades de mejora del DRP

Líder de Seguridad	- Coordinar actividades de entrenamiento, documentación y actualización del DRP. - Coordinar las actividades de pruebas del DRP. - Identificar los recursos requeridos para la operación del DRP.	- Proveer soporte a los profesionales especializados. - Notificar al proveedor de Centro de Cómputo Alterno (si aplica). - Gestionar el alistamiento y disponibilidad del Centro de Cómputo Alterno. - Coordinar con los responsables el desplazamiento al Centro de Cómputo Alterno, de los funcionarios que activarán la infraestructura. (Si aplica) - Mantener informado al Líder del DRP	- Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados.
Líder de Apoyo Logístico	- Participar en la ejecución de las pruebas al DRP	- Apoyar a los involucrados en el DRP, en actividades administrativas y logísticas ante una contingencia, entre otras. - Suministro de información de contratos. - Logística de desplazamiento, si es requerido. - Contacto de proveedores, si es requerido. - Facilitar el acceso a los insumos y suministros requeridos para que los demás roles puedan ejecutar sus responsabilidades.	- Reportar los inconvenientes y oportunidades de mejora del DRP

ACTIVIDADES DE NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL DRP

a. Las personas usuarias deben reportar el incidente a la mesa de ayuda cuando:

- NO se pueden utilizar los sistemas de información.
- NO hay red de comunicaciones.
- NO hay servicio de correo electrónico.
- NO hay acceso a los archivos electrónicos centralizados
- NO se pueden utilizar los servicios críticos de TI
- NO se puede utilizar la central telefónica
- CUALQUIER otro evento de tecnología que afecte la prestación del servicio

b. La mesa de ayuda debe atender el incidente de acuerdo con lo establecido en la gestión Soporte técnico, y se continúa con la ejecución de esta guía si:

- El incidente afecta la disponibilidad de los sistemas, a nivel general.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso al correo electrónico.
- Ningún usuario puede acceder a sus archivos electrónicos centralizados.
- El incidente afecta alguno de los servicios críticos de TI.
- En cualquiera de los casos, debe escalarlo a los funcionarios responsables, conforme el árbol de fallos.

c. El profesional especializado de la plataforma o servicio afectado debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

- Naturaleza e impacto del incidente.
- Estrategias definidas en el DRP aplicables u otras soluciones potenciales
- Tiempo estimado de solución del incidente.
- Finalmente, comunicarse con la Jefatura en Tecnologías de Información para informar los resultados del diagnóstico.

ACTIVIDADES DE MANEJO DE CRISIS O DESASTRE

A continuación, se listan las actividades y consideraciones necesarias para el manejo de una crisis que afecte o pueda afectar la reputación, imagen, u operación de la Institución.

a. Declaración de crisis o desastre:

- Se declara una crisis o desastre cuando se materializa un incidentes o problema presentados con los servicios de tecnologías de información, tales como interrupciones de los servicios en forma prolongada por más de 2 horas, falta de suministro de energía, modificación voluntaria de datos o acceso indebido a los servidores, desastres naturales, ciberataques, destrucción de equipos o incendios que afecten los Sistemas, servidores, equipos o dispositivos de la Institución.

- Se activan los escenarios de fallos que se detallan en los siguientes apartados.

b. La Jefatura de Tecnologías de Información comunica a la Presidencia Ejecutiva, teniendo en cuenta los siguientes aspectos:

- Sistemas y servicios afectados
- Resultados del diagnóstico
- Acciones realizadas

- Tiempo estimado para normalización
- Riesgos a los que está expuesta la institución por el desastre presentado, y las alternativas disponibles
- Decisiones que debe tomar la Presidencia Ejecutiva.

c. La Presidencia Ejecutiva y el Comité Institucional de Tecnologías de Información (para el Manejo de Crisis) evalúan la crisis y el impacto que puede tener para la reputación, imagen u operación de la entidad, al igual que define las acciones para afrontar la crisis.

d. Activar la atención de los diferentes escenarios

ACTIVIDADES DE MANTENIMIENTO

Es responsabilidad del Líder de Seguridad la actualización de las nuevas versiones al DRP, y la comunicación de estas a todos los funcionarios involucrados en el mismo.

La actualización y mantenimiento al DRP se debe realizar:

- Cuando ha transcurrido un año desde la última actualización.
- Cuando han ocurrido cambios en la plataforma tecnológica objeto del alcance de esta guía.
- Cuando los resultados de las pruebas requieren actualización del DRP o sus protocolos.
- Cuando hay cambios en el personal que operaría el DRP.
- Cuando los resultados de auditorías así lo indican.

ACTIVIDADES DE PRUEBA

En la realización de las pruebas al DRP están relacionadas en las siguientes actividades:
Las pruebas se realizan al menos 2 veces al año, a partir de la divulgación de esta circular, con base en las siguientes actividades:

Ciclo de pruebas anual	Descripción
Mayo	Se realizan pruebas sobre el escenario de fallo relacionado al activo de información, este consiste en pruebas de respaldos y recuperación para garantizar la integridad de los datos respaldados en al menos dos servicios críticos.
Octubre	Se realizan pruebas teniendo en consideración fallos o inconsistencias de las evaluaciones anteriores, evaluando lecciones aprendidas además de documentar las mejoras que han sido efectuadas en la infraestructura, en al menos dos servicios críticos.

CIRCULAR
INAMU-PE-009-2024
PRESIDENCIA EJECUTIVA

ESCENARIOS DE FALLAS

ATENCIÓN A ESCENARIO DE FALLOS EN LAS COMUNICACIONES.

Para una continuidad de negocios en INAMU se presentan 4 elementos que son los principales para una continuidad de operaciones de los servicios que se presta en la Plataforma Tecnológica del INAMU. En caso de fallo en las comunicaciones se deberán ejecutar estas actividades en los siguientes componentes:

FIREWALL

Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de tráfico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.

SWITCH CORE

El término switch troncal o switch core se refiere a los que se utilizan en el núcleo central (core) de las grandes redes. Es decir, a estos switches están conectados otros de jerarquía inferior, además de servidores, routers WAN.

ROUTER PRINCIPAL

Router es un dispositivo que administra el tráfico de datos que circula en una red de computadoras. Un enrutador gestiona el flujo de datos de una red local o de internet, decidiendo a qué dirección IP va a enviar el paquete de datos

PROVEEDOR DE SERVICIOS

El ICE es el proveedor de servicios del INAMU para el servicio de internet y además enlaces en cada una de las oficinas institucionales.

N	Actividad	Responsables
1	El internet está conformado por dos enlaces de 200 Mbps los cuales funcionan activo –activo formando un ancho de banda de 400 Mbps. Al haber una caída en uno de esos enlaces el otro seguirá funcionando, dando conexión a menor velocidad, pero existirá la continuidad del negocio. Con respecto a los enlaces de comunicación de las oficinas, cada una cuenta con un solo enlace el cual le da la conexión con el INAMU y el internet a la vez.	Gestor de Redes

ATENCIÓN A ESCENARIO DE FALLOS EN LOS SERVIDORES

En caso de fallo en los servidores se deberán ejecutar las siguientes actividades:

CIRCULAR
INAMU-PE-009-2024
PRESIDENCIA EJECUTIVA

ATENCIÓN A ESCENARIO DE FALLOS EN LA INFRAESTRUCTURA ELÉCTRICA

ID	Actividad		Responsables
1	Se identifican los componentes críticos los cuales serían alguno de los mencionados a continuación: • Planta de energía del edificio sigma • UPS respaldo del centro de datos		Unidad de Informática
2	Los componentes eléctricos que no se encuentre disponible debe evaluarse los tiempos que no estará disponibles.		Unidad de Informática
3	Se debe llamar al proveedor de servicios e indicar la situación.		Departamento de servicios generales
4	Se debe identificar una estrategia clara con apoyo del proveedor y servicios generales para restablecer el o los servidores caídos.		Unidad de Informática
5	Se debe verificar si la caída afectó otros equipos		Unidad de Informática
6	La estrategia debe contemplar el impacto en la infraestructura y las distintas posibilidades de recuperación		Unidad de Informática
7	Se debe ejecutar la estrategia definida.		Unidad de Informática

ATENCIÓN A ESCENARIO DE FALLOS DE LA INFRAESTRUCTURA DE CLIMATIZACIÓN

N	Actividad	Responsables
1	Primeramente, se identifican los componentes de climatización críticos los cuales serían alguno de los mencionados a continuación: • Aire acondicionado del Edificio Sigma • 2 aires acondicionados de contingencia en el Centro de Datos.	Unidad de Informática
2	Los componentes de climatización que no se encuentre disponible deben evaluarse los tiempos que no estarán disponibles.	Unidad de Informática
3	Se debe llamar al proveedor de servicios y Departamento de Servicios Generales e indicar la situación.	Departamento de servicios generales
4	Se debe identificar una estrategia clara con apoyo del proveedor para restablecer los servidores caídos.	Unidad de Informática
5	Se debe verificar si la caída ha afectado otros equipos	Unidad de Informática
6	La estrategia debe contemplar el impacto en la infraestructura y las distintas posibilidades de recuperación	Unidad de Informática
7	Se debe ejecutar la estrategia definida.	Unidad de Informática

CIRCULAR
INAMU-PE-009-2024
PRESIDENCIA EJECUTIVA

ACTIVIDADES DE RECUPERACIÓN Y CONTINGENCIA

La Unidad de Informática, cuenta con diversos protocolos a seguir para garantizar la continuidad de los servicios críticos, los cuales son:

- Protocolo de Apagado y encendido de la Plataforma Tecnológica.
- Protocolo de Continuidad de Almacenamiento
- Protocolo de Continuidad de las Bases de Datos
- Protocolo de Continuidad de los servidores
- Protocolo de Continuidad del Centro de Datos
- Protocolo de Continuidad del Servicio de TI.
- Protocolo de Seguridad y Acceso Físico al Centro de Datos
- Protocolo de Reactivación del Data Center Alterno

RECURSO HUMANO PARTICIPANTE EN EL PROCESO DE RECUPERACIÓN

Perfil / Nombre	Descripción
Líder de DRP: Ingrid Trejos Marin	Correo: itrejos@inamu.go.cr Teléfono Institucional: 2527-8494 Dirección: Edificio Sigma, San Pedro
Líder de Apoyo Logístico: Yendry Hernández Montezuma	Correo: yhernandez@inamu.go.cr Teléfono Institucional: 2527-8458 Dirección: Edificio Sigma, San Pedro
Líder de infraestructura: Jonathan Zuñiga Alvarado	Correo: jzuniga@inamu.go.cr Teléfono Institucional: 2527-8450 Dirección: Edificio Sigma, San Pedro
Líder de Mesa de ayuda (Soporte Técnico): Warner Barrantes Serrano	Correo: wbarrantes@inamu.go.cr Teléfono Institucional: 2527-8565 Dirección: Edificio Sigma, San Pedro
Líder de Seguridad: Jonathan Zuñiga Alvarado	Correo: jzuniga@inamu.go.cr Teléfono Institucional: 2527-8450 Dirección: Edificio Sigma, San Pedro
Líder de Redes y Comunicaciones: Warner Barrantes Serrano	Correo: wbarrantes@inamu.go.cr Teléfono Institucional: 2527-8565 Dirección: Edificio Sigma, San Pedro

ADILIA CARAVACA ZUÑIGA (FIRMA)

Firmado digitalmente por ADILIA CARAVACA ZUÑIGA (FIRMA)
Fecha: 2024.06.19 13:11:18 -06'00'