**Julio 2021**
**Versión: 1.1**

# Política de Procedimiento para la seguridad de los datos

EL Instituto de Conservación Forestal de la Republica de Honduras identifica la información generada por cada uno de sus colaboradores en el ejercicio de sus funciones como una parte vital y de suma importancia para la continuidad del negocio.

En función de ello se pretende dirigir las acciones y actividades tanto de sus colaboradores, de los departamentos, proyectos y demás órganos que lo integran, para lograr alcanzar un nivel de seguridad en este respecto que minimice el riesgo inherente ante los datos, su perdida, extracción y mal uso de estos.

## Objetivo:

Establecer las políticas en seguridad de la información del ICF, proporcionando el marco de referencia para su gestión en cada una de las áreas que lo integran.

## Normas específicas:

a. El Centro de datos es un espacio exclusivo para los colaboradores encargados de la administración de los servidores y demás equipos que allí se encuentran.

b. El departamento de Tecnología de la información proveerá a la organización de la infraestructura necesaria para garantizar la seguridad informática de la red del ICF.

c. La administración de los nodos que conforman la red del ICF es propia del departamento de Tecnología de la Información, por lo que la manipulación, expansión y modificación de dicha infraestructura debe ser bajo la responsabilidad de este departamento.

d. Es responsabilidad de los colaboradores del departamento Tecnología de la información de velar porque las computadoras de los funcionarios del ICF se encuentre debidamente actualizadas, que cuenten con un antivirus y un firewall que prevenga riesgos informáticos.

e. El respaldo de la información de los colaboradores, proyectos y otros órganos que integran el ICF es responsabilidad de todos los funcionarios, con la colaboración del departamento de Tecnología de la Información.

f. Las contraseñas utilizadas por los funcionarios del ICF deben de cumplir los requisitos mínimos dispuestos por el departamento de Tecnología de la información.

# Descripción del procedimiento

## Acceso al Centro de Datos

El centro de datos del ICF ubicado en su sede central, el mismo es un cuarto. El mismo cuenta con llave y es salvaguardado por un oficial de seguridad que se mantiene a pocos metros de él.

Dentro del centro de datos se encuentran racks de comunicaciones donde se ubican el switch core y la mayoría de los servidores, además de una UPS para la continuidad del flujo eléctrico en caso de falla.

El acceso al centro de datos debe de ser en compañía de alguno de los colaboradores del departamento de Tecnologías de la Información, la llave gestionada por los colaborares de T.I.

## Nodos de infraestructura

Dentro de la infraestructura tecnológica del centro se identifican diferentes nodos en los que se almacenan, transmiten e interconectan las computadoras y otros activos de la organización.

Para cada tipo de estos se especifican políticas y procedimientos de uso; en donde se asigna las responsabilidades de la gestión de estos.

La Gerencia de Tecnologías de la información cuenta en su infraestructura con un firewall, el cual tiene las reglas que regulan la seguridad de la red en cuanto a la entrada y salida de información hacia internet; este equipo deniega el trafico malintencionado, la pornografía, la violencia, el racismo, provenientes vía internet hacia las computadoras de los usuarios de la red del ICF.

Los servidores con los que cuenta la organización deben de estar ubicados dentro del centro de datos, pues es el único lugar donde se cuenta con planta eléctrica, UPS con al menos 25 minutos de carga eléctrica, doble suministro de aire acondicionado y la seguridad de acceso óptima.

En cuanto a los switch de comunicaciones la gestión, remplazo y actualización de los mismos es responsabilidad exclusiva de los colaboradores de la unidad de soporte tecnico, dichos funcionarios deben de velar por la seguridad de estos activos y mantener vigilancia de las condiciones en las que se encuentran.

La red de datos es administrada por el departamento de Tecnologías de la Información, las evaluaciones del rendimiento de esta, los planes de mantenimiento y mejora de la red son responsabilidad de la unidad de Soporte. Para la construcción de la red de datos el departamento de T.I. se apoyará de la unidad de mantenimiento del ICF o bien podrá contratar a terceros para ejecutar las labores necesarias.

## Información de la Organización y de los Usuarios

La Gerencia de Tecnologías de la Información tiene entre sus objetivos estratégicos brindar soporte a los colaboradores y aliados del ICF para mantener un nivel de seguridad adecuada, según las necesidades de los usuarios y los órganos a los que pertenece. Para lo anterior se especifica los siguientes niveles.

## Niveles de seguridad de la información

***Nivel Bajo:***

Se clasifican en este rubro la información de índole personal que podría tener un colaborador en la computadora que se le ha sido asignada para el trabajo. Con respecto a esta se le brinda colaboración para hacer los respaldos en caso de que se le vaya a sustituir la computadora o bien por su salida de la organización.

***Nivel Medio***

En este apartado se clasifica la información producida en el ejercicio de las funciones de cada uno de los colaboradores, la cual debe de estar respaldada en un medio externo. Para el respaldo se recomienda el uso del Onedrive de Microsoft que cada colaborador tiene derecho por su cuenta de usuario organizacional. En caso de que el colaborador tenga un disco duro externo para realizar sus respaldos podrá utilizarlo para ese objetivo.

***Nivel Alto***

En nivel alto se ubica la información generada por los proyectos, programas y departamento; entre estos se tienen planes anuales, políticas, procedimientos, información contable y de ejecución de los órganos que integran el ICF.

## Gestión de contraseñas

Las contraseñas utilizadas por los colaboradores del ICF para su desempeño profesional deben de ser de conocimiento estrictamente personal y en la medida de lo posible no deben de ser divulgadas a ningún otro colaborador o persona externa de la institución, no obstante, si eventualmente por razones justificadas el colaborador revela su contraseña deberá solicitar el cambio de esta.

El estándar mínimo de seguridad para las contraseñas es: contener mayúsculas, minúsculas y números, un largo mínimo de 8 caracteres y debe de ser cambiada al menos una vez al año.