Defensoría del Consumidor

SOLICITUD INICIAL DEL REQUERIMIENTO/PROYECTO

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP"

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. VIGENCIA

El presente documento entrará en vigencia ocho días hábiles posteriores a la aprobación por el (la) Presidente(a) de la Defensoría del Consumidor.

2. INSTRUCCIONES DE LLENADO

2.1 Datos Generales

Esta sección se utiliza para describir las generalidades del requerimiento/proyecto de software, donde:

Fecha y hora de solicitud, se deben colocar los valores correspondientes al momento de entrega de la solicitud a la Gerencia de Sistemas Informáticos.

Nombre de la propuesta, el nombre que tiene la propuesta debe ser auto descriptivo y suficientemente claro para evitar ambigüedades, ejemplo: Agregar un nuevo campo para registrar múltiples direcciones de notificación de un consumidor o proveedor.

Nombre del solicitante, corresponde a la persona que realiza la solicitud, la persona que será responsable de brindar la información sobre el requerimiento/proyecto o quien delegará a la(s) persona(s) que brindarán la información y acompañamiento en el proceso. Pueden ser múltiples solicitantes en caso de que el requerimiento/proyecto este compartido con otra unidad.

Cargo del solicitante, el cargo que posee la o las personas que realizan la solicitud.

Objetivo estratégico, en este apartado se debe colocar el objetivo (estratégico, POA u otros) al que pertenece este proyecto/requerimiento, en caso de que no persiga ninguno de estos objetivos se debe marcar como 'N/A'.

Área solicitante, Dirección, Unidad o Gerencia a la que pertenecen la o las personas solicitantes.

Presupuesto estimado, en caso de que el requerimiento/proyecto tenga un presupuesto asignado se debe colocar en este campo para efectos de la planificación y asignación de recursos. En caso de no poseer presupuesto se debe colocar 'N/A'.

Fecha esperada de finalización, en caso de que el requerimiento/proyecto tenga una fecha límite de implementación, se debe colocar en este campo. En caso de no poseer fecha límite se debe colocar 'N/A'.

Tipo de solicitud, se debe seleccionar el tipo de la solicitud, para ello se cuenta con dos espacios donde se debe marcar con una X según sea el caso. Las opciones disponibles son 'Nuevo sistema / Nueva funcionalidad', la cual debe ser seleccionada cuando sean nuevas características a sistemas existentes o un nuevo sistema y 'Modificación sistema existente' cuando se requieren cambios a funciones de un sistema existente.

2.2 Descripción de la Solicitud

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Esta sección se utiliza para detallar los objetivos y alcances del proyecto o requerimiento, donde:
Descripción de la situación actual, se debe describir ampliamente la situación actual, los antecedentes que dan origen a la necesidad de este requerimiento o proyecto. En esta sección se pueden colocar imágenes, documentos anexos, capturas de pantalla y todo elemento que ayude a describir el punto.

Descripción paso a paso del proceso, se debe detallar la serie de pasos que debe cumplir el requerimiento/proyecto solicitado, también se puede agregar un diagrama de procesos, flujograma, algoritmo, formulas, ecuaciones, etc.
Se debe describir de manera clara cuál es el objetivo que se pretende cumplir al realizar este proyecto/requerimiento.

Resultados esperados (criterios de aceptación), se deben listar todos aquellos elementos que se esperan como resultado de implementar el proyecto/requerimiento. En esta sección se puede colocar imágenes, documentos anexos, capturas de pantalla y todo elemento que ayude a describir el punto.

Sistemas Involucrados / Sistemas a Modificar, se deben listar todos los sistemas que se verán afectados o con los que interactuará el nuevo proyecto/requerimiento además de identificar los procesos, estados, roles, etc.

Unidades / Gerencias Involucradas, se deben listar unidades, gerencias o direcciones que se verán impactadas con este proyecto requerimiento, esto con el fin de tomarlos en cuenta en el proceso de toma de requerimientos, capacitaciones y migración de datos (en caso lo requiera).

Roles / Perfil del usuario(s) finales que utilizarán el sistema, se deben identificar las personas que utilizaran el nuevo sistema o funciones desarrolladas.

2.3. Aprobación del área solicitante

En esta sección las personas listadas en Nombre del solicitante en la sección de datos generales, deben firmar de conformidad con lo que han manifestado en la solicitud, deben firmar todas las personas solicitantes.

2.4. Visto Bueno de la Gerencia de Sistemas Informáticos

La Gerencia de Sistemas Informáticos, será la encargada de revisar la solicitud y verificar que el alcance, objetivos y resultados esperados estén claramente definidos. La GSI podrá aprobar la solicitud firmando y sellando de conformidad para luego ser remitida a presidencia o podrá realizar observaciones a la unidad solicitante.

2.5. Aprobación de Presidencia

Cuando la solicitud ha sido aprobada por la GSI, será remitida a presidencia para su aprobación definitiva, una vez aprobada la solicitud es remitida a la GSI. En caso de encontrar observaciones será remitida a la unidad solicitante.

Para de aprobar la solicitud, el (la) Presidente(a) de la DC deberá firmar y sellar la solicitud.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

3. FORMA ORIGINAL DEL FORMULARIO

SOLICITUD INICIAL DEL REQUERIMIENTO/PROYECTO

DATOS GENERALES

Fecha y hora de solicitud:		
Nombre de la propuesta:		
Nombre del solicitante:		
Cargo del solicitante:		
Objetivo estratégico:		
Área Solicitante:		
Presupuesto estimado:		
Fecha esperada de finalización:		
Tipo de solicitud:	☐ Nuevo sistema / Nueva funcionalidad	☐ Modificación sistema existente

DESCRIPCIÓN DE LA SOLICITUD

DESCRIPCIÓN DE LA SITUACIÓN ACTUAL:
DESCRIPCIÓN PASO A PASO DEL PROCESO:
OBJETIVOS DEL PROYECTO / REQUERIMIENTO:
RESULTADOS ESPERADOS (CRITERIOS DE ACEPTACIÓN):
SISTEMAS INVOLUCRADOS / SISTEMAS A MODIFICAR:
UNIDADES/GERENCIAS INVOLUCRADAS:
ROLES/PERFIL DEL USUARIO(S) FINALES QUE UTILIZARAN EL SISTEMA:

NOMBRE	CARGO	USUARIO DE SISTEMA

VERSIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

APROBACIÓN AREA SOLICITANTE

En el presente documento están definidos el alcance, características y objetivos que debe cumplir el requerimiento/proyecto solicitado. Sin más que hacer constar firmamos en muestra de aceptación, aprobación y entera satisfacción.

Aprobado por	Cargo	Firma	Fecha

VISTO BUENO DE GERENCIA DE SISTEMAS INFORMÁTICOS

Nombre	Firma	Fecha

Sello GSI

APROBACIÓN DE PRESIDENCIA

Nombre	Firma	Fecha

Sello Presidencia

VERSIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

VERSIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP.

Defensoría del Consumidor	FORMULARIO DE REGISTRO DE ENTREGA DE MALETA DE SEGURIDAD.	EL SALVADOR
	GERENCIA DE SISTEMAS INFORMÁTICOS	
	CÓDIGO: / FECHA ELABORACIÓN:	
	VERSIÓN: / PAGINA: 1 de 2	

HISTORIAL DEL DOCUMENTO.

VERSIÓN	FECHA DE MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

Elaboró:	Revisó:	Aprobó:
Gerente de Sistemas Informáticos.	Jefe de Planificación y Calidad	
Técnica de Gestión de la Calidad.	Directora de Administración	Presidenta de la Defensoría del Consumidor.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

1. VIGENCIA.

El presente documento entra en vigencia una vez sea firmado por la presidenta de la Defensoría del Consumidor.

2. INSTRUCCIONES DE LLENADO.

Este documento contiene las instrucciones para el llenado del formulario de registro de entrega de maleta de seguridad.

En el cuerpo del formulario completar la siguiente información:

- **Contenido:** Colocar la identificación de la cinta magnética (código) a resguardar en la maleta de seguridad.
- **Fecha:** Colocar la fecha en que se entrega la maleta de seguridad a la persona designada para realizar el traslado de la maleta de seguridad.
- **Entregado por:** Colocar el nombre de la persona encargada de entregar la maleta de seguridad a la persona designada para trasladarla al centro de resguardo.
- **Firma:** Colocar la firma de la persona encargada de entregar la maleta de seguridad.
- **Recibido por:** Colocar el nombre de la persona designada para trasladar la maleta de seguridad al centro de resguardo.
- **Firma:** Colocar firma de la persona designada para trasladar la maleta de seguridad al centro de resguardo.

Contenido	Fecha	Entregado por:	Firma	Recibido por:	Firma

3. FORMA ORIGINAL DEL FORMULARIO.

Defensoría del Consumidor

DEFENSORIA DEL CONSUMIDOR
Gerencia de Sistemas Informáticos
Formulario de registro de entrega de maleta de seguridad

Contenido	Fecha	Entregado por:	Firma	Recibido por:	Firma

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LA

Defensoría del Consumidor	FORMULARIO DE RESPALDO DE BASES DE DATOS EN CINTA MAGNÉTICA		EL SALVADOR
	GERENCIA DE SISTEMAS INFORMÁTICOS		
	CÓDIGO:	FECHA ELABORACIÓN:	
	VERSIÓN:	PAGINA: 1 de 4	

HISTORIAL DEL DOCUMENTO.

VERSIÓN	FECHA DE MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

Elaboró:	Revisó:	Aprobó:
Gerente de Sistemas Informáticos	Jefe de Planificación y Calidad Directora de Administración	Presidenta de la Defensoría del Consumidor.

1. VIGENCIA.
El presente documento entra en vigencia una vez sea firmado por la presidenta de la Defensoría del Consumidor.

2. INSTRUCCIONES DE LLENADO.
Este documento contiene las instrucciones para el llenado del formulario de respaldo de bases de datos en cinta magnética.

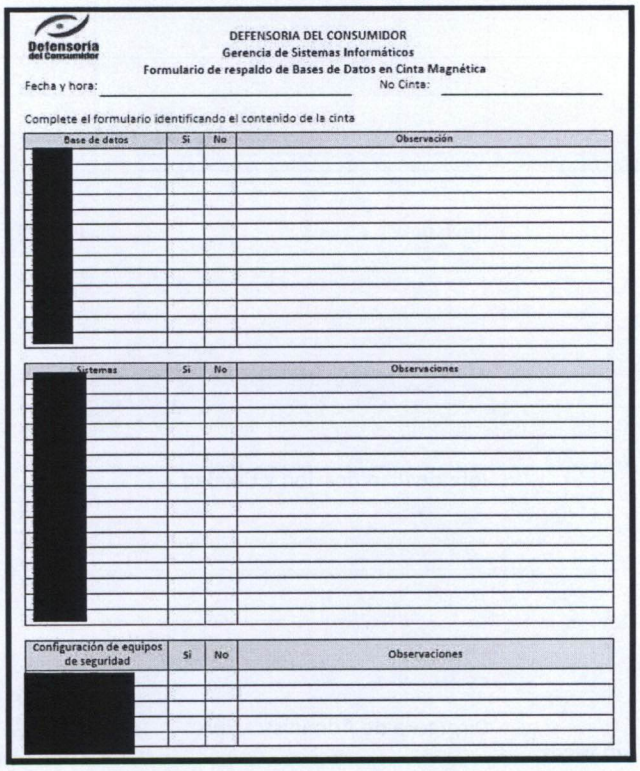
Colocar la fecha y hora en que se elabora el respaldo de bases de datos en cinta magnética y el número de la cinta magnética que se utiliza para elaborar el respaldo de base de datos.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

DEFENSORIA DEL CONSUMIDOR
Gerencia de Sistemas Informáticos
Formulario de respaldo de Bases de Datos en Cinta Magnética

Fecha y hora: _____ No Cinta: _____

Debe identificar en el formulario marcando la casilla "SI" los archivos de base de datos, sistemas de información o archivos de configuración de equipo de seguridad que hayan sido respaldados en la cinta magnética; los archivos que no hayan sido incluidos en el respaldo deberán ser identificados en el formulario marcando la casilla "NO".



DEFENSORIA DEL CONSUMIDOR
Gerencia de Sistemas Informáticos
Formulario de respaldo de Bases de Datos en Cinta Magnética

Fecha y hora: _____ No Cinta: _____

Complete el formulario identificando el contenido de la cinta

Base de datos	Si	No	Observación
[redacted]			

Sistemas	Si	No	Observaciones
[redacted]			

Configuración de equipos de seguridad	Si	No	Observaciones
[redacted]			

Colocar el nombre y la firma de la persona encargada de realizar el respaldo de base de datos y la persona encargada de verificar que el respaldo de base de datos que se realizó corresponda a lo que señalado en el formulario.

Realizado por:	Verificado por:
Firma:	Firma:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

3. FORMA ORIGINAL DEL FORMULARIO.

Defensoría del Consumidor

DEFENSORÍA DEL CONSUMIDOR
Gerencia de Sistemas Informáticos
Formulario de respaldo de Bases de Datos en Cinta Magnética

Fecha y hora: _____ No Cinta: _____

Complete el formulario identificando el contenido de la cinta

Base de datos	Si	No	Observación
[redacted]			

Sistemas	Si	No	Observaciones
[redacted]			

Configuración de equipos de seguridad	Si	No	Observaciones
[redacted]			

Realizado por:	Verificado por:
Firma:	Firma:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO.

VERSIÓN	FECHA DE MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

Elaboró:	Revisó:	Aprobó:
Gerente de Sistemas Informáticos.	Jefe de Planificación y Calidad	
Técnica de Gestión de la Calidad.	Directora de Administración	Presidenta de la Defensoría del Consumidor.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

1. VIGENCIA.
El presente documento entra en vigencia una vez sea firmado por la Presidenta de la Defensoría del Consumidor.

2. INSTRUCCIONES DE LLENADO.
Este documento contiene las instrucciones para el llenado del formulario de entrega de cintas.

En el cuerpo del formulario completar la siguiente información:
- **Fecha:** Colocar la fecha en que se almacena la cinta magnética en el centro de resguardo.
- **Número de la cinta:** Colocar el correlativo correspondiente a la cantidad de cintas que se trasladarán al Centro de resguardo.
- **Nombre de etiqueta:** Colocar el identificador de la cinta magnética a resguardar (código).
- **Tipo de Unidad:** Colocar el tipo de medio magnético en el que se traslada el respaldo.
- **Observaciones:** Colocar comentarios sobre el traslado del respaldo.
- **Sello Institucional:** Colocar el sello de la Unidad organizativa que realiza el traslado.

Fecha:

DESCRIPCIÓN DE CINTAS		
Numero de Cinta	Nombre de etiqueta	Tipo de Unidad

Observaciones:	Sello Institucional

La persona encargada de realizar el respaldo de base de datos en la cinta magnética, debe colocar su nombre, firma y hora en que se realiza el respaldo.

Nombre del encargado de realizar el respaldo	Firma	Hora

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

La persona encargada de verificar que la cinta magnética donde se realizó el respaldo de base de datos corresponda a la cinta a trasladar al centro de resguardo, debe colocar su nombre, firma y la hora de realizar la verificación.

Nombre de la persona que verifica el respaldo	Firma	Hora

La persona designada para trasladar al centro de resguardo la cinta magnética en la cual se realizó el respaldo de bases de datos, debe colocar su nombre, firma y hora que en que se traslada la cinta al centro de resguardo.

Nombre de persona que transporta cintas	Firma	Hora

La persona del centro de resguardo quien es el (la) encargado(a) de la bóveda de seguridad externa, debe colocar su nombre, firma y hora en que se reguarda la cinta magnética en la bóveda.

Nombre del encargado/a Bóveda de seguridad externa	Firma	Hora

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso, así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

3. FORMA ORIGINAL DEL FORMULARIO.

Defensoría del Consumidor

Entrega de Cintas

Fecha:

DESCRIPCIÓN DE CINTAS		
Numero de Cinta	Nombre de etiqueta	Tipo de Unidad

Observaciones:	**Sello Institucional**

Nombre del encargado de realizar el respaldo	Firma	Hora
Nombre de la persona que verifica el respaldo	Firma	Hora
Nombre de persona que transporta cintas	Firma	Hora
Nombre del encargado/a Bóveda de seguridad externa	Firma	Hora

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

HOJA DE MANTENIMIENTO PREVENTIVO

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. VIGENCIA

El presente documento entrará en vigencia ocho días hábiles posteriores a la aprobación por el (la) Presidente(a) de la Defensoría del Consumidor.

2. INSTRUCCIONES DE LLENADO

El presente documento contiene las instrucciones para el llenado la hoja de mantenimiento preventivo.

a) Colocar el nombre de la persona encargada del equipo al cual se le brindó mantenimiento preventivo.
b) Colocar la Unidad Organizativa (Dirección, Subdirección) / área o unidad.
c) Colocar el N° del inventario del equipo al cual se le brindó mantenimiento preventivo
d) Colocar la fecha en que se ha programó el mantenimiento preventivo del recurso informático.
e) Colocar la fecha real en que se proporcionó el mantenimiento preventivo al recurso informático.
f) Seleccionar las condiciones finales del equipo luego del mantenimiento preventivo.
g) Colocar el nombre de la persona que realizó el mantenimiento preventivo.
h) Colocar el nombre de el (la) técnico(a) de la Gerencia de Sistemas Informáticos (GSI) que verificó el mantenimiento

Para el mantenimiento de computadora:

i) Seleccionar los componentes identificados en el equipo.
j) Seleccionar las actividades realizadas en hardware.
k) Seleccionar las actividades realizadas en software

Para el mantenimiento de impresor:

l) Seleccionar las actividades realizadas en hardware

Para el mantenimiento de Escáner

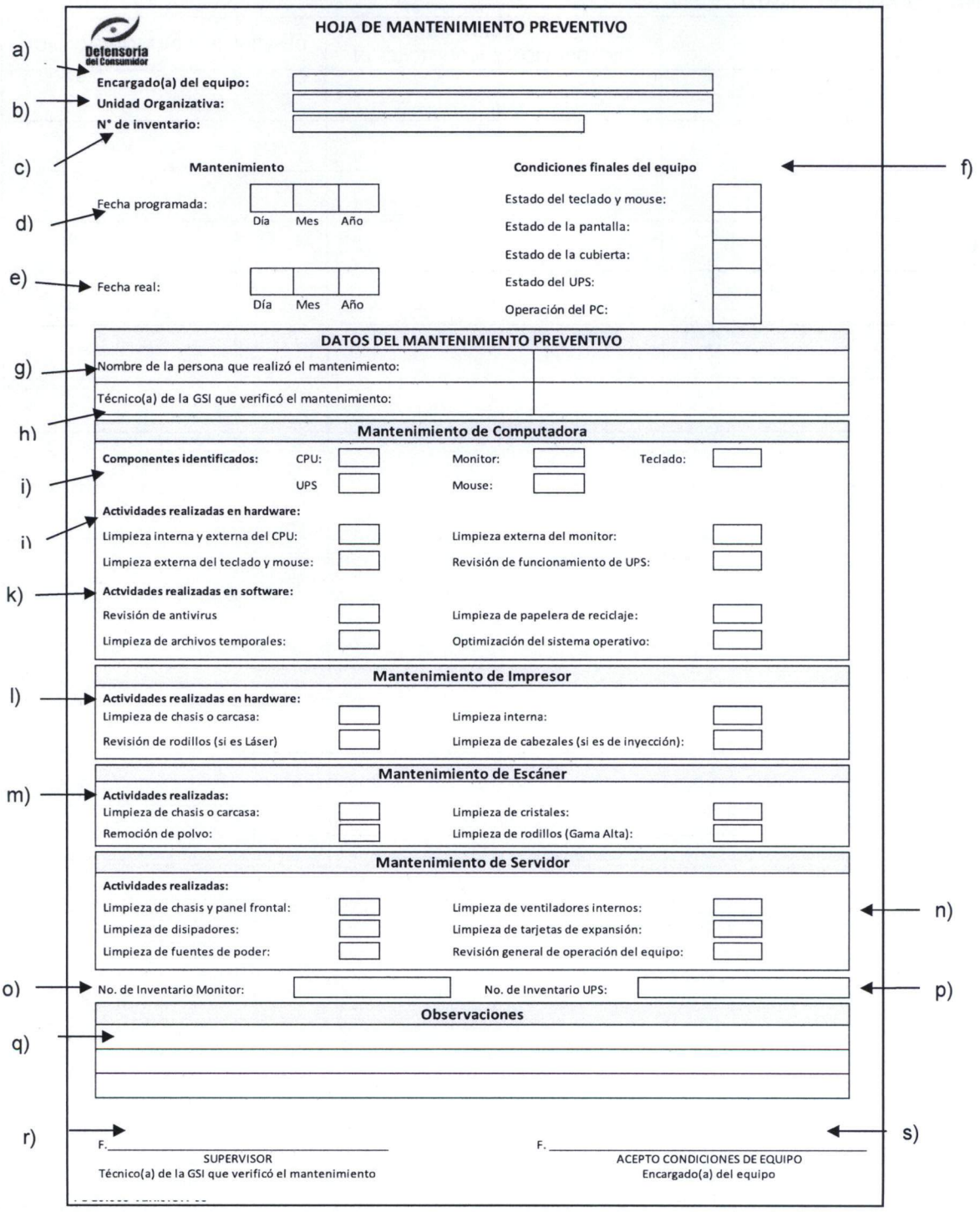
m) Seleccionar las actividades realizadas.

Para el mantenimiento de servidor:

n) Seleccionar las actividades realizadas
o) Colocar el N° del inventario del monitor al cual se brindó mantenimiento preventivo.
p) Colocar el N° del inventario del UPS al cual se brindó mantenimiento preventivo.
q) En caso que existan observaciones el técnico de la Gerencia de Sistemas Informáticos debe colocar las que considere oportunas.
r) Colocar firma de el (la) técnico(a) de la GSI que verificó el mantenimiento preventivo.
s) Colocar firma de el (la) usuario(a) del equipo informático al cual se brindó mantenimiento preventivo.

3. FORMA ORIGINAL DEL FORMULARIO

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP"



HOJA DE MANTENIMIENTO PREVENTIVO

Defensoría del Consumidor

a) **Encargado(a) del equipo:**

b) **Unidad Organizativa:**

N° de inventario:

c)

Mantenimiento

d) Fecha programada: Día Mes Año

e) Fecha real: Día Mes Año

Condiciones finales del equipo ← f)

Estado del teclado y mouse:
Estado de la pantalla:
Estado de la cubierta:
Estado del UPS:
Operación del PC:

DATOS DEL MANTENIMIENTO PREVENTIVO

g) Nombre de la persona que realizó el mantenimiento:

Técnico(a) de la GSI que verificó el mantenimiento:

h)

Mantenimiento de Computadora

Componentes identificados: CPU: Monitor: Teclado: UPS Mouse:

i)

Actividades realizadas en hardware:

j) Limpieza interna y externa del CPU: Limpieza externa del monitor:
Limpieza externa del teclado y mouse: Revisión de funcionamiento de UPS:

k) **Actvidades realizadas en software:**

Revisión de antivirus: Limpieza de papelera de reciclaje:
Limpieza de archivos temporales: Optimización del sistema operativo:

Mantenimiento de Impresor

l) **Actividades realizadas en hardware:**

Limpieza de chasis o carcasa: Limpieza interna:
Revisión de rodillos (si es Láser) Limpieza de cabezales (si es de inyección):

Mantenimiento de Escáner

m) **Actividades realizadas:**

Limpieza de chasis o carcasa: Limpieza de cristales:
Remoción de polvo: Limpieza de rodillos (Gama Alta):

Mantenimiento de Servidor

Actividades realizadas:

Limpieza de chasis y panel frontal: Limpieza de ventiladores internos: ← n)
Limpieza de disipadores: Limpieza de tarjetas de expansión:
Limpieza de fuentes de poder: Revisión general de operación del equipo:

o) No. de Inventario Monitor: No. de Inventario UPS: ← p)

Observaciones

q)

r) F._____ ← s) F. _____

SUPERVISOR
Técnico(a) de la GSI que verificó el mantenimiento

ACEPTO CONDICIONES DE EQUIPO
Encargado(a) del equipo

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor	FORMULARIO PARA TRASLADO DE ACTIVO FIJO POR REPARACIÓN	EL SALVADOR
	GERENCIA DE SISTEMAS INFORMÁTICOS	
	CÓDIGO: / FECHA ELABORACIÓN:	
	VERSIÓN: / PAGINA: 1 de 3	

HISTORIAL DEL DOCUMENTO.

VERSIÓN	FECHA DE MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

Elaboró:	Revisó:	Aprobó:
Gerente de Sistemas Informáticos.	Jefe de Planificación y Calidad	
Técnica de Gestión de la Calidad.	Directora de Administración	Presidenta de la Defensoría del Consumidor.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

1. VIGENCIA.
El presente documento entra en vigencia una vez sea firmado por la Presidenta de la Defensoría del Consumidor.

2. INSTRUCCIONES DE LLENADO.
Este documento contiene las instrucciones para el llenado del formulario para traslado de activo fijo por reparación.

Cuando el equipo informático sea trasladado por reparación se deberán completar con letra legible los siguientes campos del formulario:

- **FECHA DE TRASLADO.** Colocar la fecha en que se traslado el equipo informático a reparación.
- **EQUIPO.** Indicar el nombre del tipo de equipo que se retirara (cpu, monitor, ups, tablet, impresor o escáner).
- **MARCA.** Colocar la marca del equipo informático a trasladar.
- **MODELO.** Colocar el modelo del equipo informático a trasladar.
- **SERIE.** Colocar la serie de fabricación del equipo informático a trasladar.
- **NUMERO DE INVENTARIO.** Colocar el número de inventario que la Defensoría del Consumidor ha asignado al equipo que se trasladara para reparación.
- **NOMBRE DEL ENCARGADO DEL EQUIPO.** Colocar el nombre de la Persona que tiene asignado el equipo informático a retirar.
- **MOTIVO DEL TRASLADO.** Indicar el motivo por el cual el equipo se le retirara al usuario.
- **FIRMA DE LA PERSONA ENCARGADA DEL ACTIVO FIJO.** Colocar firma de la persona que tiene asignado el equipo informático a reparar.
- **NOMBRE Y FIRMA DE LA PERSONA QUE RECIBE EL ACTIVO FIJO.** Colocar el nombre y firma de la persona que retira el equipo para reparación.

Cuando el equipo informático que se retiró por reparación sea devuelto al usuario se deberán completar con letra legible los siguientes campos:

- **FECHA DE ENTREGA.** Colocar la fecha en que se devuelve al usuario el equipo informático que se encontraba en reparación.
- **ESTADO DEL BIEN.** Indicar el estado en que se entrega el equipo informático.
- **DETALLE DE REPARACIÓN.** Colocar específicamente que reparación o prueba se le realiza al equipo informático que se retiro.
- **NOMBRE Y FIRMA DE LA PERSONA QUE ENTREGA EL ACTIVO FIJO.** Colocar el nombre y firma de la persona que entrega el equipo informático reparado.
- **NOMBRE Y FIRMA DE LA PERSONA QUE RECIBE EL ACTIVO FIJO.** Colocar el nombre y firma de la persona que tiene asignado el equipo informático reparado.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

3. FORMA ORIGINAL DEL FORMULARIO.

Defensoría del Consumidor	FORMULARIO PARA TRASLADO DE ACTIVO FIJO POR REPARACIÓN FOGSI002 VERSION 01				FECHA DE TRASLADO
EQUIPO:		MARCA:		MODELO:	
SERIE:		N° DE INVENTARIO:			
NOMBRE DEL ENCARGADO DEL EQUIPO:					
MOTIVO DEL TRASLADO:					
NOMBRE Y FIRMA DE LA PERSONA ENCARGADA DEL ACTIVO FIJO		NOMBRE Y FIRMA DE LA PERSONA QUE RECIBE EL ACTIVO FIJO			
DEVOLUCION DEL EQUIPO					
FECHA DE ENTREGA:		ESTADO DEL BIEN:			
DETALLE DE REPARACIÓN:					
NOMBRE Y FIRMA DE LA PERSONA QUE ENTREGA EL ACTIVO FIJO		NOMBRE Y FIRMA DE LA PERSONA QUE RECIBE EL ACTIVO FIJO			

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

PLAN ANUAL DE MANTENIMIENTO PREVENTIVO

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidenta de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Directora de Administración Jefe de Planificación y Calidad

1. VIGENCIA.
El presente documento entra en vigencia ocho días hábiles posteriores a la aprobación por el (la) Presidente(a) de la Defensoría del Consumidor

2. INSTRUCCIONES DE LLENADO.
El Plan anual de Mantenimiento Preventivo contiene los aspectos para realizar el mantenimiento preventivo del equipo informático de la Defensoría del Consumidor, a continuación, se detallan las instrucciones de llenado:

a) En la portada del plan anual de mantenimiento preventivo colocar el año en que se elabora.

I. **Firma y fecha de aprobación**. Este apartado será completado por el (la) Director(a) Administrativo(a) al momento de dar por aprobado el Plan de Mantenimiento Preventivo de recurso informático

b) El contenido del plan está compuesto por 7 aspectos que a continuación se detallan:

I. **Diagnostico situacional**. En este apartado se debe listar la cantidad de equipo informático (computadoras, UPS) por oficina que posee la Defensoría del Consumidor.
NOTA: Las computadoras, UPS que se consideren deben estar debidamente inventariadas y no debe ser equipo en alquiler.

II. **Objetivos.** Colocar los objetivos generales y específicos que se desean alcanzar al realizar el mantenimiento preventivo del equipo informático.

*Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP

III. **Responsabilidades y ámbito de aplicación.** Se debe colocar la unidad organizativa responsable de ejecutar el plan de mantenimiento preventivo y vigilar por el cumplimiento de los objetivos definidos.

IV. **Estructura del plan.** En este apartado el plan debe considerar la siguiente información:

1. Colocar el nombre y cargo de las personas responsables de realizar y de ejecutar el plan de mantenimiento preventivo.
2. Indicar los componentes de hardware (CPU, monitor, teclado, mouse, UPS) a los cuales se brindará mantenimiento y las principales actividades a realizar al momento de ejecutar el mantenimiento.
3. Indicar las principales actividades que comprende el mantenimiento preventivo de software del equipo de cómputo.

V. **Cronograma de ejecución.** Colocar en un cronograma las fechas en que se tiene estimado iniciar el mantenimiento preventivo en cada una de las oficinas de la Defensoría del Consumidor.

NOTA: El cronograma puede colocarse como un anexo al plan de mantenimiento y hacer referencia a dicho anexo en este apartado.

VI. **Recursos necesarios.** Definir el recurso material y el número de estudiantes de servicio social se necesitaran como mínimo para ejecutar el plan de mantenimiento preventivo.

VII. **Seguimiento y monitoreo.** Indicar la persona responsable de monitorear la ejecución del plan y de proporcionar un informe detallado al Gerente de Sistemas Informáticos sobre el plan ejecutado.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

3. FORMA ORIGINAL DEL FORMULARIO.

Portada

Defensoría del Consumidor

Plan de mantenimiento preventivo de recurso informático

Dirección de Administración
Gerencia de Sistemas Informáticos

Año ____

Firma y fecha de aprobación
Director(a) Administrativo(a)

Este documento presenta la planificación de actividades para la realización del mantenimiento preventivo de equipos de la Defensoría del Consumidor, detallando los requerimientos necesarios, responsabilidades, recurso humano y cronograma de actividades a ejecutar.

El mantenimiento correctivo se realizará de acuerdo a los requerimientos recibidos.

FOGSI001 VERSIÓN 02

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Página inicial

1

FOGSI001 VERSIÓN 02

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTYO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP"

Defensoría
del Consumidor

RESPALDO DE DOCUMENTOS ESCANEADOS Y ARCHIVOS UBICADOS EN LOS EQUIPOS ASIGNADOS A EMPLEADOS DE LA INSTITUCIÓN

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. BASE LEGAL

Normas técnicas de control interno específicas de la Defensoría del Consumidor, Art. 65.

2. OBJETIVO

Establecer los lineamientos necesarios para realizar el respaldo de documentos escaneados y archivos que se encuentran en las computadoras asignadas a los(las) empleados(as) de la Defensoría del Consumidor, para efectos de proteger la información y asegurar la continuidad y el restablecimiento oportuno de los Sistemas de Información, en caso de eventos que pudieran interrumpir el logro de los objetivos Institucionales.

3. ALCANCE

El presente documento aplica para:

- Todos los documentos escaneados que se registren a través del Sistema de Control de Documentos Digitales.
- Los archivos de trabajo que se encuentran en las computadoras asignadas al personal de la Defensoría del Consumidor que se requiera respaldar.

4. VIGENCIA

El presente documento entrará en vigencia una vez transcurridos ocho días hábiles desde la aprobación por el(la) Presidente(a) de la DC.

5. REFERENCIAS NORMATIVAS

Norma General para la Elaboración de Documentos Normativos.

6. RESPONSABLE

El(La) responsable de la aplicación de esta norma es el(la) Gerencia de Sistemas Informáticos.

7. DEFINICIONES Y TERMINOLOGÍA

Contingencia: Posibilidad de que una cosa suceda o no suceda.

Oficina: diversas ubicaciones de la Defensoría del Consumidor (Centro de Solución de Controversias, Dirección de Vigilancia de Mercado, Regional San Miguel, Regional Santa Ana, Plan de la Laguna).

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Respaldo: copia de los archivos en una ubicación separada de modo que se puedan restaurar si le pasara algo a la computadora, o si fueran borrados accidentalmente.

Rutina: acto repetitivo.

Servidor de archivos: es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.

8. REQUISITOS

8.1. RESPALDO DE DOCUMENTOS ESCANEADOS REGISTRADOS EN EL SISTEMA DE CONTROL DE DOCUMENTOS DIGITALES

8.1.1. Para elaborar el respaldo de documentos escaneados, debe existir la rutina en el servidor de archivos que genere el respaldo de estos documentos de forma automática y con una programación establecida.

8.1.2. El respaldo debe ser realizado una vez al día y debe trasladarse hacia el servidor de respaldo de archivos ubicado en el sitio de contingencia.

8.1.3. La rutina de respaldo debe registrar el resultado de cada respaldo.

8.2. RESPALDO DE ARCHIVOS UBICADOS EN LOS EQUIPOS ASIGNADOS A EMPLEADOS DE LA INSTITUCIÓN

8.2.1. Debe existir un listado de equipos a los cuales se desea realizar el respaldo. El listado debe ser elaborado y aprobado por la Jefatura del área solicitante, y ser remitido a la Gerencia de Sistemas Informáticos.

8.2.2. Para elaborar el respaldo de archivos, debe existir la rutina en cada uno de las computadoras en las cuales se ha solicitado realizar el respaldo, la cual debe generar el respaldo de forma automática y con una programación establecida.

8.2.3. Debe existir una carpeta llamada "RESPALDO" la cual será ubicada en la carpeta "Mis documentos" en cada una de las computadoras identificada en el listado de equipos a los cuales se desea que se realice el respaldo

8.2.4. El respaldo debe realizarse una vez al día y debe ser trasladado hacia el servidor de respaldo de archivos ubicado en la oficina donde se encuentra la computadora a la cual se realiza el respaldo.

8.2.5. La rutina de respaldo debe registrar el resultado de cada respaldo.

8.2.6. Se debe contar con una aplicación para realizar el respaldo de archivos de forma automática.

9. ANEXOS

No Aplica.

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

USO DE CONTRASEÑAS

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. BASE LEGAL
ISO 27001, anexo A, A.11.3.1 Uso de Contraseñas

2. OBJETIVO
Establecer los lineamientos para regular la creación y uso de contraseñas robustas, cuando éste sea el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios de la Defensoría del Consumidor (DC).

3. ALCANCE
El presente documento es de aplicación y de obligatorio cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la DC, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la DC y utilicen contraseñas como medio de autenticación personal.

4. VIGENCIA
El presente documento entrará en vigencia una vez transcurridos ocho días hábiles desde la aprobación por el(la) Presidente(a) de la DC.

5. REFERENCIAS NORMATIVAS
NOUPYC003 Norma General para la Elaboración de Documentos Normativos.

6. RESPONSABLE
El(La) Usuario(a): es responsable de custodiar debidamente las claves y contraseñas que se suministren para el acceso a sistemas o servicios de la DC, impidiendo el uso indebido o acceso por parte de terceros.

Director(a) de Administración: será responsable de velar por el cumplimiento de éste documento.

Gerente(a) de Sistemas Informáticos (GSI): será responsable de velar por el cumplimiento de la presente norma en lo relacionado a los controles que garantizan la confidencialidad e integridad de las contraseñas.

7. DEFINICIONES Y TERMINOLOGÍA
Contraseña: código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Personal de organizaciones externas: Talento humano que forma parte de estructuras administrativas y sistemas administrativos creadas para lograr metas u objetivos, que no son parte de la DC.

8. REQUISITOS

Uso de contraseñas

8.1. Las contraseñas son de uso personal y por ningún motivo se deberán prestar o facilitar a otros(as) usuarios(as).

8.2. Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

8.3. Las contraseñas no se deberán escribir en ningún medio, excepto cuando son generadas por primera vez por la GSI o entregadas en custodia.

8.4. Las contraseñas de usuario(a) de sistema operativo y de aplicaciones [cuentas del Sistema de Atención de Reclamos y Asesorías (SARA), cuentas de correo electrónico, cuentas de servicios Web, intranet, entre otros] deberán cambiarse cada 90 días. Además, deberá cambiarse siempre que el usuario(a) sospeche que la seguridad de su contraseña puede estar comprometida.

8.5. Los(Las) usuarios(as) deberán cambiar las contraseñas la primera vez que usen la cuenta asignada.

Selección y custodia de contraseñas

8.6. La seguridad de este tipo de autenticación se basa en dos premisas:

a. La contraseña personal solo la conoce el(la) usuario(a).
b. La contraseña es lo suficientemente "fuerte" para no ser descifrada.

8.7. La contraseña para ser considerada "fuerte" (segura) debe poseer las siguientes características:

a. Debe tener como mínimo 8 caracteres.
b. Utiliza caracteres de tres de los cuatro grupos siguientes y siempre que uno de ellos deberá ser un símbolo:
   i. Letras minúsculas
   ii. Letras mayúsculas
   iii. Números (por ejemplo, 1, 2, 3).
   iv. Símbolos (por ejemplo, ¡, @, #, =, - *, etc.)

8.8. La contraseña no debe ser, ni derivarse de una palabra de diccionario, de la jerga o de un dialecto.

8.9. La contraseña no debe derivarse del nombre de el(la) usuario(a) o de un pariente cercano.

8.10. La contraseña no debe derivarse de información personal (del número de teléfono, número de DUI, fecha de nacimiento, etc.) de el(la) usuario(a) o de un pariente cercano.

8.11. Las contraseñas no podrán contener 3 o más caracteres consecutivos del nombre de el(la) usuario(a) o del nombre completo de la persona.

8.12. No debe utilizar la misma contraseña que utiliza para las cuentas de recursos y servicios institucionales en otras cuentas (acceso a su proveedor de servicios personal, acceso a servicios de su banco, entre otros).

8.13. No debe compartir las cuentas y contraseñas con nadie. Todas las contraseñas deben ser tratadas como información sensible y confidencial.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

8.14. No debe revelar su contraseña por teléfono a nadie, incluso aunque reciba una solicitud en nombre del personal de la GSI o de un superior en la institución.

8.15. Nunca escriba la contraseña en papel. Tampoco almacene contraseñas en archivos de computadora sin encriptar o proveerlo de algún mecanismo de seguridad.

8.16. No debe revelar su contraseña a sus superiores, ni a sus colaboradores.

8.17. No hable sobre una contraseña delante de otras personas.

8.18. No revele su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.

8.19. No comparta la contraseña con familiares.

8.20. No debe revelar la contraseña a sus compañeros(as) cuando se ausente de la institución.

8.21. No debe utilizar la característica de "Recordar Contraseña" existente en algunas aplicaciones (Outlook, Internet Explorer, Chrome).

8.22. Debe reportarse a la GSI cualquier sospecha que una persona esté utilizando la contraseña y una cuenta que no le pertenece.

Estándar para el desarrollo de aplicaciones

8.23. La GSI deberá asegurar los mecanismos de autenticación utilizados en el desarrollo de sistemas institucionales, garantizando que los sistemas desarrollados contienen las siguientes precauciones en términos de seguridad respecto a la selección y uso de contraseñas:

a. No deben almacenar contraseñas en texto claro o en ninguna forma fácilmente reversible
b. Deben proveer de algún tipo de mecanismo de roles, de forma que un(a) usuario(a) pueda tomar las funciones de otro sin necesidad de conocer la contraseña del anterior.
c. Deben proveer de un mecanismo para expirar las contraseñas y obligar a los(las) usuarios(as) al cambio de la misma.
d. Se debe limitar el número de intentos de accesos sin éxito consecutivos.
e. Debe proveer un mecanismo de notificación a el(la) propietario(a) de la cuenta para los casos en que sobrepase el número de intentos de acceso sin éxito consecutivos.

Infracciones y sanciones

8.24. El incumplimiento de la presente norma puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la DC.

8.25. Las jefaturas aplicarán lo dispuesto en el Reglamento Interno de Trabajo que rige al personal de la Institución, en el caso de incumplimiento de la presente norma.

9. ANEXOS

No aplica

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

USO DE CORREO ELECTRÓNICO INSTITUCIONAL

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. BASE LEGAL

Reglamento para el uso y control de las tecnologías de información y comunicación en las entidades del sector público, Art. 28

2. OBJETIVO

Establecer los lineamientos necesarios para regular el uso del correo electrónico institucional utilizado por el personal de la Defensoría del Consumidor (DC).

3. ALCANCE

El presente documento debe ser conocido y cumplido por todo el personal de la DC, tanto por personal interno como externo que utilicen el servicio de correo electrónico institucional de la DC, sea cual fuere su nivel jerárquico.

4. VIGENCIA

El presente documento entrará en vigencia una vez transcurridos ocho días hábiles desde la aprobación por el(la) Presidente(a) de la DC.

5. REFERENCIAS NORMATIVAS

Norma General para la Elaboración de Documentos Normativos.
Uso de contraseñas.

6. RESPONSABLE

El(La) Usuario(a): será responsable de utilizar el servicio de correo electrónico institucional para los propósitos declarados en el presente documento. Es total y completamente responsable por los correos que de su cuenta sean enviados.

Los(Las) Jefes(as), Directores(as) y Gerentes(as): deben asegurarse que el personal bajo su cargo conoce y da cumplimiento a éste documento.

Director(a) de Administración: será responsable de velar por el cumplimiento de este documento.

Gerente(a) de Sistemas Informáticos: será responsable de velar por el normal funcionamiento del servicio de correo electrónico. Así como también de monitorear el uso que los(las) empleados(as) hacen de este servicio, en los

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

casos en que se detecte algún empleado haciendo uso indebido, se notificará inmediatamente a el(la) Jefe(a) inmediato(a).

7. DEFINICIONES Y TERMINOLOGÍA

Correo electrónico: servicio de mensajería provisto a los(las) empleados(as) de la DC para facilitar la comunicación y gestión de la institución.

Usuario(a): toda persona que utilice de manera directa o indirecta un servicio provisto por un recurso computacional.

SPAM: mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Pirámide o estafa piramidal: es un esquema de negocios en el cual los(las) participantes recomiendan y captan (refieren) a más clientes(as) con el objetivo de que los(las) nuevos(as) participantes produzcan beneficios a los(las) participantes originales.

Phishing: es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Relaying: es la acción de utilizar un servidor como medio de difusión de correo electrónico en el cual, el(la) remitente o el(la) destinatario(a) no son usuarios(as) de dicho servidor.

CPU: es el hardware dentro de una computadora u otro dispositivo programable, que interpreta las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema.

Caracter especial: Se refiere a caracteres que no forman parte del repertorio estándar, entre ellos se encuentran: #,*,&, ¥, §, µ, æ, entre otros.

Código Hostil: Es una variedad de formas que engloba el término código malicioso, entre ellas los virus informáticos, gusanos, troyanos, la mayoría de los rootkits y los programas espías (spyware).

Rootkits: Es un conjunto de software que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

Buenas costumbres: Se refiere al conjunto de normas sociales que no alteran el orden público, preservando la paz y la seguridad, encontrándose estrechamente asociado a otros conceptos éticos y morales, tales como la decencia, el decoro, la dignidad y el pudor.

8. REQUISITOS

La DC declara que el servicio de correo electrónico es un recurso que la Institución pone a disposición de los(las) empleados(as) como una herramienta de trabajo, por el que se invierten recursos para mantener el servicio activo. Por tanto, la DC podrá regular el uso del correo electrónico y exigir a los(las) usuarios(as) internos(as) y externos(as) a la DC el cuidado y uso correcto de este servicio.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

La Gerencia de Sistemas Informáticos, un mes antes de renovar el servicio, hará una revisión de las cuentas de correo electrónico para deshabilitar las que no se estén utilizando, con el objetivo de hacer eficiente el uso de los recursos y pago de suscripciones.

8.1. Ante ello, la DC declara que: toda casilla de correo electrónico directamente vinculada a una persona en específico, es decir, donde la dirección de correo esté vinculada con el nombre y apellido de el(la) usuario(a), será considerada con carácter de correspondencia privada, siendo su uso exclusivamente con fines laborales.

8.2. El contenido es considerado privado, su uso debe ser solo con fines laborales. En consecuencia, el uso del correo electrónico no debe ser para fines personales o particulares.

8.3. El correo electrónico tiene por finalidad, facilitar y agilizar la comunicación entre las unidades de la DC y con entidades externas con las cuales tiene relación por su naturaleza de trabajo

8.4. El(La) responsable de cada Unidad, Dirección, Gerencia o Jefatura será el(la) encargado(a) de solicitar el alta o baja del correo electrónico institucional para el personal que esté a su cargo. La Unidad de Talento Humano, deberá notificar a la Gerencia de Sistemas Informáticos, sobre el personal que deje de laborar en la institución por cualquier motivo.

8.5. La solicitud de creación del correo electrónico institucional deberá realizarse conforme al Procedimiento "Creación de cuenta de correo electrónico" mediante el formulario para solicitar la creación de cuentas de correo electrónico ().

8.6. El(La) usuario(a) para quien se pretenda registrar su alta en el servicio de correo electrónico, deberá contar con equipo de cómputo, con al menos la configuración básica para acceder a la red institucional de la DC.

8.7. El correo electrónico debe identificar en la firma: nombre, apellido, unidad interna a la que pertenece, número de teléfono y número de teléfono celular institucional en caso le haya sido asignado, para conocimiento de los mismos por parte del destinatario. La Gerencia de Sistemas Informáticos (GSI) entregará a cada empleado(a) la información relativa a la firma en formato imagen estandarizada o generada a través del servidor de correo electrónico.

8.8. Las credenciales de acceso, son personales e intransferibles.

8.9. La contraseña deberá contener como mínimo 8 caracteres alfanuméricos, entre ellos al menos una letra mayúscula y al menos un carácter especial (condición para formar la contraseña). Como medida de seguridad se solicitará automáticamente el cambio de contraseña cada tres meses.

8.10. En el caso que un(a) usuario(a) olvide su contraseña o sospeche que otras personas están accediendo a su cuenta de correo electrónico, deberá notificarlo inmediatamente a la GSI para solicitar cambio de contraseña.

8.11. El límite de almacenamiento por buzón de correo electrónico es de 5 GB (Gigabytes). En caso exceda este límite, será notificado por la Jefatura de la GSI mediante correo electrónico, para que depure el buzón de la cuenta asignada. De hacer caso omiso a la notificación, no recibirá correos.

8.12. El límite para enviar y recibir archivos adjuntos es de 15 MB, salvo en casos excepcionales y que el(la) responsable del área presente la debida justificación a la GSI.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

8.13. En caso que la cuenta de correo deje de ser utilizada por un período de 6 meses, la GSI enviará notificación a el(la) responsable del área para determinar el proceso de baja definitiva de la cuenta del servidor de correo electrónico.

Asignación de cuentas de correo electrónico

8.14. Toda cuenta de correo electrónico creada:

8.14.1. Pertenecerá a el(la) usuario(a) para quién se solicitó, no se deberá asignar cuentas de correo de tipo genéricas o de acceso múltiples.

8.14.2. Deberá estar protegida con contraseña de acceso. Será responsabilidad de el(la) usuario(a) tener su contraseña en lugar seguro y no debe ser nunca una contraseña de dominio público.

8.14.3. Únicamente los(as) empleados(as) y personal externo autorizado poseerán cuentas de correo electrónico en los servidores de la institución. El alta o baja de las cuentas de correo electrónico para personal externo deben ser solicitadas mediante el formulario para solicitar la creación de cuentas de correo electrónico (), por el(la) Director(a), Jefe(a) o Gerente(a) encargado(a) del área donde se desempeñará el personal.

Cuentas de correo grupal

8.15. Existen grupos de correo electrónico que concentran las cuentas de correo electrónico de los(las) empleados(as) ubicados(as) en cada una de las oficinas de la Institución:

- Oficina Plan de la Laguna:
- Oficina Dirección de Vigilancia de Mercado:
- Oficina Centro de Solución de Controversias San Salvador:
- Oficina Regional de Occidente:
- Oficina Regional de Oriente:

8.16. Existe una cuenta de correo electrónico que agrupa las cuentas de correo de los Jefes(as), Gerentes(as), Directores(as), Asesores(as) y Presidencia, la cuenta grupal tiene por nombre

8.17. Las cuentas de correo electrónico grupales, definidas en el numeral 8.15. y 8.16, son de uso exclusivo para Presidencia, Asesores(as), Directores(as), Gerentes(as) o Jefaturas.

8.18. Existe una cuenta de correo que agrupa a todo el personal de la institución, tiene por nombre y es de uso exclusivo de Presidencia de la institución y es moderada por la Unidad de Comunicaciones.

8.19. Existe una cuenta de correo electrónico, que agrupa a todo el personal de la institución, tiene por nombre y es de uso exclusivo de Dirección Administrativa, Unidad Financiera Institucional, Unidad de Talento Humano y la Gerencia de Sistemas Informáticos y es moderada por la Jefatura de la Dirección Administrativa.

Acceso a correo electrónico a través de Internet

8.20. La Institución pone a disposición el acceso al correo electrónico a través de internet, con el objetivo de mejorar la comunicación con los(las) funcionarios(as) que por misión oficial o personal estén fuera de la Institución. El acceso al correo interno institucional será a través de la dirección

Responsabilidad de los(las) usuarios(as) con sus cuentas de correo electrónico

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

8.21. El(La) usuario(a) es total y completamente responsable por los correos que de su cuenta sean enviados, por la razón antes expuesta las contraseñas deben estar guardadas en lugar seguro, y deberán ser conocidos únicamente por la persona poseedora de la cuenta de correo.

8.22. Durante el proceso de entrega de la cuenta de correo electrónico a cada empleado(a), éste(a) firmará un acuerdo en el cual hace constar que recibe la cuenta de correo electrónico, que conoce las cuentas grupales de la institución y que conoce la normativa para el uso del correo electrónico institucional. El acuerdo además detallará la capacidad de almacenamiento de la cuenta de correo electrónico y la capacidad máxima (en MB) para el envío de archivos adjuntos.

8.23. Cuando el(la) usuario(a) tenga configurado el correo electrónico en un dispositivo móvil, y éste sea hurtado o robado, deberá notificar inmediatamente a la Gerencia de Sistemas Informáticos y ésta validará la información correspondiente, para ejecutar procedimiento en el servidor cuando se tenga acceso, lo cual permitirá el restablecimiento de fábrica del dispositivo, es decir borrará la información que se tenía en el dispositivo, siempre y cuando tenga acceso a internet, posteriormente deberá seguir los pasos establecidos en el acta de entrega de asignación del dispositivo móvil.

Capacidad del servidor para cada cuenta de correo

8.24. La Gerencia de Sistemas Informáticos garantizará un servicio de correos capaz de soportar la carga de los(las) usuarios(as) que la DC posee, asegurando así la continuidad de las operaciones.

8.25. Todo(a) usuario(a) deberá tener una cuota de espacio dentro del servidor de correos.

Casos excepcionales para acceder al correo electrónico de un(a) usuario(a)

8.26. La DC podrá acceder al contenido del correo electrónico de sus empleados(as) y usuarios(as) externos(as), solo en los siguientes casos excepcionales:

8.26.1. Fallecimiento.

8.26.2. Desvinculación laboral de el(la) empleado(a) (ejemplo: retiro voluntario, despido, etc.) donde debe existir una entrega de la cuenta de correo electrónico durante el proceso de inventario formal.

8.26.3. Enfermedad temporal o definitiva de el(la) empleado(a) o usuario(a) externo(a) que no le permita acceder al correo electrónico.

8.26.4. Expresa voluntad de el(la) empleado(a), previamente autorizado por escrito y con visto bueno o aprobación de el(la) Jefe(a) inmediato(a).

8.27. En todos los casos mencionados, deberá informarse a el(la) Auditor(a) Interno(a) sobre la solicitud de acceso a contenido de correo electrónico, documentando el motivo y la aceptación por parte de el(la) usuario(a) de la cuenta de correo electrónico.

8.28. Se aclara que el fin de este acceso excepcional es el de permitir que la unidad a la cual pertenece el(la) usuario(a), pueda continuar sus labores habituales.

8.29. Todo requerimiento fuera de esta declaración será considerado como información de carácter de reserva total por un período de 7 años. La información permanecerá almacenada en el servidor de correo electrónico institucional, será la GSI la encargada de velar por la disponibilidad, integridad y confidencialidad de la información almacenada.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Uso inaceptable

8.30. Se prohíbe el envío mediante correo electrónico de toda publicidad o cualquier otro tipo de aviso comercial no solicitado previamente por el(la) destinatario(a).

8.31. Se prohíbe el envío mediante correo electrónico de toda cadena de correos, hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "Cartas en cadena", "Pirámides", "Phishing" o enviar correo electrónico solicitando donaciones caritativas, peticiones de firmas o cualquier material relacionado.

8.32. Se prohíbe brindar servicios que, de manera directa o indirecta, faciliten la proliferación de SPAM o "correo electrónico masivo no solicitado". En esto se incluye casillas de correo, software para realizar SPAM, hosting de sitios Web para realizar SPAM o que realicen SPAM.

8.33. Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del orden público, la moral, las buenas costumbres nacionales e internacionales y los usos y costumbres aplicables en internet, y el respeto de los derechos fundamentales de las personas.

8.34. Se prohíbe el envío de contenido ilegal por naturaleza (todo lo que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, pornografía, amenazas, estafas, virus o código hostil en general.

8.35. Se prohíbe el envío de mensajes masivos que comprometan la reputación u honra de la organización o de alguno de sus miembros.

8.36. Se prohíbe la utilización de servidores de correo distintos a los servidores de la DC, para emitir correo con identificación de dominios de la DC.

8.37. Se prohíbe el envío de un número alto de mensajes por segundo que tenga el objetivo de dificultar o paralizar el servicio de correo electrónico ya sea por saturación de las redes, de la capacidad de CPU del servidor u otro.

8.38. Se prohíbe utilizar un servidor de correo para retransmitir correo sin el permiso expreso del sitio (Relaying).

8.39. Se prohíbe falsificar encabezados de correos electrónicos, utilizar nombres de dominio que sean inválidos o inexistentes, u otras formas engañosas de enviar correo electrónico.

8.40. Se prohíbe personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal.

8.41. Material pornográfico, chistes, música, videos, fotografías personales, y todo material que comprometa los principios de otras personas, no debe ser enviado por correo electrónico, las sanciones para este caso se consultarán en el reglamento interno de la DC.

8.42. Las cadenas de la suerte, temas de religión, noticias mal intencionadas y todo material obtenido de internet o de fuentes poco fidedignas, no debe ser tratada por el correo interno de la DC, esto puede causar pérdida de confianza y de credibilidad a la institución y causa tráfico innecesario en los servidores y otros equipos designados para el desarrollo de las actividades diarias de la institución.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la

8.43. En ningún momento se deberá hacer uso del correo electrónico interno de la institución para comprometer la integridad moral de la misma, o para comprometer los ideales contra los que fue creada, el uso de correo electrónico estará estrictamente destinado para mejorar la comunicación dentro y fuera de la institución, cualquier material que no esté relacionado a las labores diarias, podrá estar sujeto a supervisión por parte de la GSI, cualquier sanción al respecto deberá ser tratada de acuerdo al reglamento interno de la institución.

Infracciones y sanciones

8.44. En los casos en que la GSI identifique y compruebe el incumplimiento a ésta norma, se notificará por medio escrito a el(la) Director(a), Gerente(a) o Jefe(a) de la Unidad a la cual pertenezca la persona propietaria de la cuenta de correo electrónico involucrada, a el(la) Director(a) Administrativo(a) y a el(la) Auditor(a) Interno(a).

8.45. Se sancionará administrativamente a todo(a) empleado(a) que viole lo dispuesto en la presente norma de uso de correo electrónico, conforme a lo dispuesto por Reglamento Interno de Trabajo que rige al personal de la institución.

9. ANEXOS

No aplica.

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidenta de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Elaboró:	Revisó:
	Directora de Administración Interina Ad honorem
Gerente de Sistemas Informáticos Interino Ad honorem	Jefe de Planificación y Calidad

1. BASE LEGAL

Ley de Acceso a la Información Pública.

2. OBJETIVO

Establecer el lineamiento general para regular el uso de dispositivos de almacenamiento externo en los equipos de cómputo de la Defensoría del Consumidor (DC).

3. ALCANCE

El presente documento es de aplicación y de obligatorio cumplimiento para todo el personal que de manera permanente o eventual preste sus servicios en la DC, incluyendo el personal de organizaciones externas, cuando sean usuarios(as) o posean acceso a equipos de cómputo de la DC.

4. VIGENCIA

El presente documento entrará en vigencia ocho días hábiles posteriores a la aprobación por el(la) Presidente(a) de la DC.

5. REFERENCIAS NORMATIVAS

No aplica.

6. RESPONSABLE

Gerente(a) de Sistemas Informáticos: será responsable de velar por el cumplimiento de la presente norma en lo relacionado a los controles que garantizan el uso regulado de dispositivos de almacenamiento externo.

Director(a) de Administración: será responsable de velar por el cumplimiento de este documento.

El(La) Empleado(a): será responsable de dar cumplimiento a esta normativa.

Los(as) Jefes(as), Directores(as) y Gerentes(as): deben asegurarse que el personal bajo su cargo conoce y da cumplimiento a éste documento.

7. DEFINICIONES Y TERMINOLOGÍA

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

CD: es un formato estándar para almacenamiento de datos en discos compactos.

DVD: es un tipo de disco óptico para almacenamiento de datos.

USB: es una interfaz que permite, a través de su puerto, conectar todo tipo de dispositivos y periféricos a una computadora.

Memoria flash USB: es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información.

SD Card: es un dispositivo en formato de tarjeta de memoria para dispositivos portátiles. Sus variantes **miniSD** y **microSD** se pueden utilizar, también directamente, en ranuras SD mediante un adaptador.

Disco duro externo: es una unidad de disco duro que es fácil de instalar y transportar de una computadora a otra, sin necesidad de consumir constantemente energía eléctrica o batería.

Usuario(a): toda persona que utilice de manera directa o indirecta un servicio provisto por un recurso computacional.

8. REQUISITOS

Uso de dispositivos de almacenamiento externo

8.1 Con carácter general, el uso de dispositivos de almacenamiento externo en las unidades de la DC no está autorizado.

8.2 Por razones de seguridad de la información, las interfaces USB y la escritura en CD/DVD de las computadoras asignadas al personal de la DC estarán deshabilitados.

8.3 En caso que se requiera, la autorización de habilitar el acceso a medios de almacenamiento externo, el(la) Director(a), Gerente(a) o Jefe(a) de cada área, deberá proporcionar el nombre de el(la) empleado(a) que tiene asignado el equipo, el número de inventario de la computadora, tipo de medio de almacenamiento y la justificación que respalda dicho requerimiento.

8.4 Los dispositivos de almacenamiento externo están destinados para ser utilizados como herramienta de transporte de archivos y no como herramienta de almacenamiento.

8.5 La DC pondrá a disposición de los(las) empleados(as) aplicaciones, servicios y sistemas para almacenamiento en red y que podrán utilizarse de manera alternativa para compartir archivos entre usuarios(as).

8.6 La pérdida de un dispositivo de almacenamiento externo que contenga información institucional deberá hacerse del conocimiento de la dirección, gerencia o jefatura correspondiente y de la Gerencia de Sistemas Informáticos (GSI) por medio escrito detallando el contenido de la información.

Medidas a aplicar

8.7 En los casos en que la GSI identifique y compruebe el incumplimiento a esta norma, se notificará por medio escrito a el(la) Director(a), Gerente(a) o Jefe(a) de la unidad a la cual pertenezca el(la) empleado(a) y a el(la) Director(a) de Administración.

8.8 Se sancionará administrativamente a todo(a) empleado(a) que viole lo dispuesto en la presente norma de uso de dispositivos USB, conforme a lo dispuesto por Reglamento Interno de Trabajo que rige al personal de la institución.

9. ANEXOS

No aplica.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

USO DE EQUIPO INFORMÁTICO

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. BASE LEGAL

Manual de Organización y Funciones, , apartado 3.2 Responsabilidades Generales al Puesto, a) Hacer buen uso y documentar los traslados de los activos fijos asignados a su puesto.
Normas técnicas de control interno específicas de la Defensoría del Consumidor.

2. OBJETIVO

Establecer los lineamientos necesarios para un uso adecuado de equipo informático.

3. ALCANCE

El presente documento debe ser conocido y cumplido por todo el personal de la Defensoría del Consumidor (DC), tanto por personal interno como externo que hagan uso de equipo informático de la DC, sea cual fuere su nivel jerárquico.

4. VIGENCIA

El presente documento entra en vigencia ocho días hábiles posteriores a la aprobación por el(la) Presidente(a) de la Defensoría del Consumidor.

5. REFERENCIAS NORMATIVAS

Uso de dispositivos de almacenamiento externo V01.

6. RESPONSABLE

El(La) Usuario(a): Será responsable de hacer un buen uso del equipo informático al que tenga acceso

Los(Las) Jefes(as), Directores(as) y Gerentes(as): Deberán asegurarse que el personal bajo su cargo conoce y de cumplimiento a este documento.

Director(a) de Administración: Será el responsable de velar por el cumplimiento de este documento.

Gerente(a) de Sistemas Informáticos: Será responsable de velar por el cumplimiento del buen uso de equipo informático de la DC.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la

Coordinador(a) de Infraestructura Tecnológica y Técnico(a) de Soporte de Sistemas Informáticos: Serán responsables de verificar que el equipo informático, al cual se le brinde mantenimiento preventivo y/o correctivo no presente indicios de un mal uso del equipo informático, de lo contrario se dejará reflejado en el documento de mantenimiento y se le notificará al jefe(a) inmediato(a).

7. DEFINICIONES Y TERMINOLOGÍA

Usuario(a): Toda persona que utilice de manera directa equipo informático.

Equipo Informático: Se entenderá por equipo informático lo siguiente: Computadora u ordenador de escritorio, Computadora u ordenador portátil, escáner de computadora, impresora y todo equipo tecnológico que se utilice para el trabajo asignado.

Computadora u ordenador de escritorio: Es un dispositivo electrónico para el procesamiento de datos compuesto básicamente de CPU, monitor, teclado, ratón procesador, memoria y dispositivos de entrada/salida, y permite procesar información.

Computadora u ordenador portátil: Es una computadora personal portátil alimentada por una batería o un cable de CA enchufado a una toma eléctrica, que también se usa para cargar la batería. Las computadoras portátiles tienen un teclado adjunto, trackpad o joystick isométrico que realizan las funciones de un mouse para navegación. Una computadora portátil también tiene una pantalla o monitor delgada que se adjunta y se puede doblar para el transporte, contiene el microprocesador, memorias RAM, disco duro y en algunos casos unidad óptica de lectura/escritura y demás electrónica para procesar e interpretar las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema.

CPU: Es el hardware compuesto en su interior por un microprocesador principal, memorias RAM, disco duro y en algunos casos cuentan con unidades ópticas de lectura y escritura. Su función principal es procesar e interpretar las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema.

Monitor: Es un dispositivo electrónico de salida de la computadora en el que se muestran las imágenes y textos generados por medio de un adaptador gráfico o de video de ésta. su función principal y única es la de permitir al usuario interactuar con la computadora.

Teclado y ratón: Son los dispositivos periféricos de entrada, uno utiliza una disposición de botones o teclas, para que actúen como palancas mecánicas en el caso del teclado y el otro actúa como un dispositivo apuntador utilizado para facilitar el manejo de un entorno gráfico.

Escáner de computadora: Es un periférico que se utiliza para "copiar", mediante el uso de la luz, imágenes impresas o documentos a formato digital (a color o a blanco y negro).

Impresora: Es un dispositivo periférico del ordenador que permite producir una gama permanente de textos o gráficos de documentos almacenados en un formato electrónico, imprimiéndolos en medios físicos, normalmente en papel, utilizando cartuchos de tinta o tecnología láser (con tóner).

Hardware: Componentes físicos del equipo informático.

Software: Componentes lógicos del equipo informático.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

8. REQUISITOS

8.1. El inventario de equipo informático debe estar debidamente actualizado por la Unidad de Logística – Activo Fijo, es decir asignado a la persona que utiliza directamente el equipo.

8.2. El equipo informático que se utilice de manera directa y no esté asignado al usuario(a), se considerará responsable del equipo informático.

9. USO ADECUADO DE COMPUTADORA U ORDENADOR DE ESCRITORIO

9.1. Encender la computadora ejerciendo presión moderada en el botón de ON (Encendido)/OFF (Apagado) con un dedo de la mano.
9.2. Si el equipo pide actualizaciones o se actualiza durante el arranque del sistema operativo espere el tiempo que sea necesario hasta que finalicen las actualizaciones.
9.3. Si conecta dispositivos de almacenamiento externo (debe tener la autorización según NOGSI004 Uso de Dispositivos de Almacenamiento Externo) de dudosa procedencia, recuerde que puede contener software que vulnere los sistemas informáticos.
9.4. Si come sobre el teclado u otro dispositivo periférico, puede dañar las partes electrónicas.
9.5. Si usa depósitos con líquidos, puedan derramarse sobre el CPU y sus periféricos
9.6. Si coloca objetos sobre el CPU y sobre sus periféricos, pueden dañarlos por el peso, por la obstrucción de ventilación, por deterioro de las partes o por proliferación de plagas de insectos o roedores.
9.7. Abrir el CPU, únicamente lo debe de realizar personal de la Gerencia de Sistemas Informáticos, el sustraer elementos internos, se notificará a la jefatura correspondiente.
9.8. Evitar la descarga de archivos desde sitios web desconocidos que pudieran contener software o material potencialmente peligroso para la computadora y la seguridad de la red institucional.
9.9. Mantener la computadora apagada mientras no está en uso.
9.10. Apagar la computadora haciendo clic en la opción de apagar desde el sistema operativo.
9.11. El desconectar el cable de poder para apagar el equipo, podría dañar el sistema operativo.
9.12. En caso de presentar fallas se deberá reportar a través de la mesa de servicio (GLPI). La Gerencia de Sistemas Informáticos serán encargados de diagnosticar el problema y/o brindar una solución o realizar gestiones con proveedores.
9.13. El uso correcto a los equipos de informáticos es necesario para garantizar su correcto funcionamiento y extender su vida útil.

10. USO ADECUADO DE COMPUTADORA U ORDENADOR PORTÁTIL

10.1. Encender la computadora ejerciendo presión moderada en el botón de ON (Encendido)/OFF (Apagado) con un dedo de la mano.
10.2. Si el equipo pide actualizaciones o se actualiza durante el arranque del sistema operativo espere el tiempo que sea necesario hasta que finalicen las actualizaciones.
10.3. Si conecta dispositivos de almacenamiento externo (debe tener la autorización según NOGSI004 Uso de Dispositivos de Almacenamiento Externo) de dudosa procedencia, recuerde que puede contener software que vulnere los sistemas informáticos.
10.4. Si come sobre el teclado u otro dispositivo periférico, puede dañar las partes electrónicas.
10.5. Si usa depósitos con líquidos, pueden derramarse sobre la computadora y dañar las partes electrónicas.
10.6. Desarmar la computadora, únicamente lo debe de realizar personal de la Gerencia de Sistemas Informáticos, el sustraer elementos internos, se notificará a la jefatura correspondiente.
10.7. Evitar la descarga de archivos desde sitios web desconocidos que pudieran contener software o material potencialmente peligroso para la computadora y la seguridad de la red institucional.
10.8. El desconectar el cable de poder para apagar el equipo, podría dañar el sistema operativo.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

10.9. Conectarse a redes inalámbricas libres (redes inseguras que no piden contraseña) o redes inalámbricas en lugares públicos, puede comprometer la seguridad ya que la comunicación podría ser vulnerada.
10.10. En caso de presentar fallas se deberá reportar a través de la mesa de servicio (GLPI). La Gerencia de Sistemas Informáticos serán encargados de diagnosticar el problema y/o brindar una solución o realizar gestiones con proveedores.
10.11 El uso correcto a los equipos de informáticos es necesario para garantizar su correcto funcionamiento y extender su vida útil.
10.12. Mantener la computadora apagada mientras no está en uso o en ahorro de energía.
10.13. Apagar la computadora haciendo clic en la opción de apagar desde el sistema operativo.
10.14. Son exclusiva responsabilidad del empleado, no debe prestarse a terceros ni darle un uso que no sea afín del trabajo institucional.
10.15. Si se traslada equipo fuera de la oficina de la Defensoría del Consumidor, debe realizar la documentación correspondiente y tomar las medidas de seguridad por robo o hurto de equipo.
10.16. Evitar las temperaturas ambientes extrema.
10.17. Evitar dejar la computadora sobre objetos que obstaculicen el funcionamiento de los ventiladores, puede conducir a un sobrecalentamiento.
10.18. Evitar la descarga de la batería por debajo del 40%.

11. USO ADECUADO IMPRESORA

11.1. Si toca las partes internas de la impresora, sin conocimientos técnicos podrían dañar las partes importantes de la misma.
11.2. El forzar la salida de papel tirando de él, podría dañar los rodillos de la impresora. De igual manera si usa o reutilizar papel con polvo, arrugado o grapado.
11.3. Para evitar que le ingrese polvo, cubrirla mientras no se esté utilizando.
11.4. Si utiliza papel reciclado, debe de asegurarse de que el papel no lleve grapas, clips, polvillo u otro elemento que pueda dañar los rodillos internos de la impresora.

12. USO ADECUADO ESCÁNER DE COMPUTADORA

12.1. Si toca las partes internas, sin conocimientos técnicos, se podrían dañar las partes importantes del mismo.
12.2. Para evitar que le ingrese polvo, cubrirla mientras no se esté utilizando.

13. USO ADECUADO DE TABLET

13.1. Si coloca objetos pesados sobre la misma, se podrían dañar o quebrar la pantalla.
13.2. Utilizar franela de micro fibra para la limpieza de la misma.
13.3. Evitar la descarga de archivos desde sitios web desconocidos e instalación de aplicaciones no autorizadas que pudieran contener material potencialmente peligroso para la tablet y la seguridad de la red institucional.
13.4. Conectarse a redes inalámbricas libres (redes inseguras que no piden contraseña) o redes inalámbricas en lugares públicos, puede comprometer la seguridad ya que la comunicación podría ser vulnerada.
13.5. En caso de presentar fallas se deberá reportar a través de la mesa de servicio (GLPI). La Gerencia de Sistemas Informáticos serán encargados de diagnosticar el problema y/o brindar una solución o realizar gestiones con proveedores.
13.6 El uso correcto a los equipos de informáticos es necesario para garantizar su correcto funcionamiento y extender su vida útil.
13.7. Son exclusiva responsabilidad del empleado, no debe prestarse a terceros ni darle un uso que no sea afín del trabajo institucional.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

13.8. Si se traslada equipo fuera de la oficina de la Defensoría del Consumidor, debe realizar la documentación correspondiente y tomar las medidas de seguridad por robo o hurto de equipo.

14. ANEXOS

No aplica.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN/MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

PROCEDIMIENTO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DEL RECURSO INFORMÁTICO

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el p. proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LA.

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. BASE LEGAL
Norma Técnica de Control Interno específicas para la Defensoría del Consumidor, artículos 54.

2. OBJETIVO
Establecer los lineamientos necesarios para realizar el mantenimiento preventivo y correctivo del recurso informático de la Defensoría del Consumidor (DC), para mantenerlo en óptimas condiciones de operación y prolongar su vida útil.

3. ALCANCE
El presente procedimiento aplica a todo el recurso informático de la DC al cual se le realizará mantenimiento preventivo y/o correctivo.

4. VIGENCIA
El presente documento entrará en vigencia una vez transcurridos ocho días hábiles desde la aprobación por el(la) Presidente(a) de la DC.

5. REFERENCIAS NORMATIVAS
NOUPYC003 Norma General para la Elaboración de Documentos Normativos.

6. RESPONSABLE
El (la) responsable de la aplicación de este procedimiento es el(la) Gerente(a) de Sistemas Informáticos.

7. DEFINICIONES Y TERMINOLOGÍA
Hardware: Conjunto de elementos tangibles que componen un ordenador, impresor, servidor, router, switch, etc. y que formen parte de un equipo dichos componentes pueden ser: monitor, impresoras, CPU, periféricos, cables, tarjetas u otro tipo de elemento o partes tangibles de un equipo.

Mantenimiento Correctivo: Conjunto de acciones puntuales que se realizan a raíz del uso, agotamiento de la vida útil, u otros factores externos, de elementos que conforman el recurso informático permitiendo su restauración o recuperación.
Mantenimiento Preventivo: Conjunto de acciones de carácter periódico y permanente que tienen la particularidad

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

de proveer acciones anticipadas al deterioro del uso y agotamiento de la vida útil de elementos que conforman el equipo informático.

Recurso Informático: Son los componentes tangibles (hardware) y programas (software) que son necesarios para el buen funcionamiento de un ordenador.

Software: Es el conjunto de elementos intangibles de un ordenador. Es el conjunto de programas, datos e instrucciones lógicas necesarias para hacer posible la realización de una tarea específica.

8. REQUISITOS

8.1. Para elaborar el Plan de Mantenimiento Preventivo del recurso informático, el inventario de equipo informático de la DC debe estar debidamente actualizado.

8.2. El Plan Anual de Mantenimiento Preventivo del recurso informático deberá ser aprobado durante el último trimestre del año.

8.3. El mantenimiento preventivo del recurso informático se realizará anualmente y se iniciará su ejecución a partir del último trimestre del año y se extiende hasta el siguiente año.

8.4. La realización del mantenimiento preventivo del recurso informático se coordinará con el(la) Director(a), Gerente(a) o Jefe(a) de cada unidad organizativa para disponer de los equipos sin afectar sus labores cotidianas.

8.5. El mantenimiento preventivo se realiza al recurso informático que no posea garantía vigente.

8.6. El mantenimiento preventivo es realizado y supervisado por personal técnico de la Gerencia de Sistemas Informáticos, con el apoyo de estudiantes en servicio social de la carrera de técnico en mantenimiento de computadoras o áreas afines.

8.7. El mantenimiento preventivo y correctivo del recurso informático que se encuentre en arrendamiento, debe estar condicionado a lo establecido en el documento legal (contrato) que ampare dicho recurso informático.

9. PASOS

9.1. MANTENIMIENTO PREVENTIVO

El(La) Gerente(a) de Sistemas Informáticos

9.1.1. Genera el inventario de todo el recurso informático de la Defensoría del Consumidor.

9.1.2. Elabora el Plan de Mantenimiento Preventivo del recurso informático ().

9.1.3. Envía el Plan Mantenimiento Preventivo del recurso informático () a el(la) Director(a) de Administración para su aprobación.

El(La) Director(a) de Administración

9.1.4. Recibe y revisa el Plan de Mantenimiento Preventivo del recurso informático ().

9.1.5. Si no existen observaciones al Plan de Mantenimiento Preventivo del recurso informático (), lo aprueba y gira instrucciones a el(la) Gerente(a) de Sistemas Informáticos para iniciar su ejecución.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

9.1.6. Si existen observaciones al Plan de Mantenimiento Preventivo del recurso informático (), remite las observaciones a el(la) Gerente(a) de Sistemas Informáticos para que realice los cambios necesarios.

El(La) Gerente(a) de Sistemas Informáticos

9.1.7. Recibe el Plan de Mantenimiento Preventivo del recurso informático aprobado.

9.1.8. Gestiona con la Unidad de Talento Humano el apoyo de estudiantes en servicio social para la ejecución del Plan de Mantenimiento Preventivo.

9.1.9. Realiza las evaluaciones, teórica (Anexo 1) y práctica (Anexo 2) a los (as) estudiantes interesados(as) en realizar el servicio social, se toma como parámetro de aceptación a los(as) estudiantes que cumplan con una calificación mayor o igual a 7.

9.1.10. Informa a la entidad educativa sobre el resultado de las evaluaciones y selecciona a los(as) estudiantes que apoyarán en la ejecución del Plan.

9.1.11. Se archivan los resultados de las evaluaciones realizadas a los(as) estudiantes examinados.

9.1.12. De acuerdo a la cantidad de estudiantes seleccionados(as), se revisa la programación del mantenimiento preventivo y en caso de ser necesario se ajusta la programación.

9.1.13. Se asigna a el(la) Coordinador(a) de Infraestructura Tecnológica el seguimiento a la ejecución del Plan de Mantenimiento Preventivo, se entrega la programación y el listado de los(as) estudiantes que han sido seleccionados.

9.1.14. Coordina con los(las) Directores(as), Gerentes(as) y Jefes(as) de cada unidad organizativa la fecha en que se realizará el mantenimiento preventivo al recurso informático de su unidad.

El(La) Coordinador(a) de Infraestructura Tecnológica

9.1.15. Gestiona solicitud de transporte, cuando el recurso informático al cual se brindará mantenimiento preventivo se encuentre ubicado fuera de las oficinas del Plan de la Laguna de la Defensoría del Consumidor.

9.1.16. Supervisa la ejecución de las actividades definidas para el mantenimiento preventivo al recurso informático.

9.1.17. Asigna a un(a) Técnico(a) de Soporte de la Gerencia de Sistemas Informáticos la ejecución y verificación del Mantenimiento Preventivo en cada área, la asignación de técnicos podrá variar dependiendo de la disponibilidad de cada técnico(a).

El (La) Técnico(a) de Soporte de la Gerencia de Sistemas Informáticos

9.1.18. Supervisa y ejecuta las actividades definidas para el mantenimiento preventivo al recurso informático.

9.1.19. Verifica las pruebas de funcionamiento del equipo luego de realizarse el mantenimiento, si no existen fallas entrega el recurso informático a el(la) usuario(a) y gestiona la firma de recepción del servicio a través de la lista de control de mantenimiento preventivo y el formulario.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP"

9.1.20. Si existen fallas en el recurso informático, informa a el(la) Coordinador(a) de Infraestructura Tecnológica sobre la falla, procede a retirar el equipo y completa el formulario para traslado de activo fijo por reparación () y lo entrega a la persona que tiene a cargo el equipo.

9.1.21. Realiza la reparación del equipo.

9.1.22. Si la falla es corregida, entrega recurso informático a el(la) usuario(a), solicita el formulario para traslado de activo fijo por reparación () y se gestiona la firma de recepción del servicio, si no es posible corregir la falla elabora un informe sobre la falla y la entrega a el(la) Coordinador(a) de Infraestructura Tecnológica.

El(La) Coordinador(a) de Infraestructura Tecnológica

9.1.23. Informa a el(la) Gerente(a) de Sistemas Informáticos sobre la falla del equipo y entrega copia del informe.

El(La) Gerente(a) de Sistemas Informáticos

9.1.24. Elabora memorándum sobre la falla del equipo y lo envía a el(la) Director(a) /Gerente(a) /jefe(a) del área al cual pertenece el equipo.

El(La) Usuario(a)

9.1.25. Recibe recurso informático luego del mantenimiento preventivo y verifica su correcto funcionamiento y firma la hoja de mantenimiento preventivo (FOGSI003); si el recurso informático se retiró por reparación firma el formulario para traslado de activo fijo por reparación (FOGSI002) y lo entrega a el(la) técnico(a) de soporte de sistemas informáticos.

El(La) Técnico(a) de Soporte de Sistemas Informáticos

9.1.26. Archiva la hoja de mantenimiento preventivo () y el formulario para traslado de activo fijo () en caso haya sido necesario.

El(La) Coordinador(a) de Infraestructura Tecnológica

9.1.27. Prepara y entrega un informe detallado sobre el trabajo realizado en la ejecución del Plan a el(la) Gerente(a) de Sistemas Informáticos

El(La) Gerente(a) de Sistemas Informáticos

9.1.28. Notifica a través de memorándum a la Unidad de Talento Humano sobre la finalización del servicio social e informa los resultados del mismo.

9.2. MANTENIMIENTO CORRECTIVO

El(La) Usuario(a)

9.2.1. Reporta de forma verbal, correo electrónico o por medio del sistema de incidentes a el(la) Técnico(a) de Soporte de la Gerencia de Sistemas Informáticos la falla en el recurso informático (hardware y/o software).

El(La) Técnico(a) de Soporte de Sistemas Informáticos/Técnico(a) de Desarrollo de Sistemas Informáticos

9.2.2. Registra en el Sistema de incidentes las características de la falla reportada.

9.2.3. Verifica si existen incidencias de la misma falla reportadas por el (la) usuario(a).

9.2.4. Contacta a el(la) usuario(a) e intenta atender la falla de forma remota, si no es posible programa la atención in situ.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP"

9.2.5. Gestiona solicitud de Transporte, si la falla reportada ocurre fuera de las oficinas del Plan de La Laguna de la Defensoría del Consumidor.

9.2.6. Acude con el(la) usuario(a), revisa el recurso informático (hardware y/o software) y realiza diagnóstico para determinar el motivo de la falla. Se evalúa si el equipo debe ser retirado y se completa el formulario para traslado de activo fijo por reparación ().

9.2.7. Toma las acciones correspondientes para reparar el recurso informático (Hardware y/o Software) y solventar la falla.

9.2.8. Realiza pruebas de funcionamiento en presencia de el(la) usuario(a) con la finalidad de verificar que la falla fue solventada.

9.2.9. Si no es posible corregir la falla elabora un informe y la entrega a el(la) Coordinador(a) de Infraestructura Tecnológica.

El(La) Coordinador(a) de Infraestructura Tecnológica

9.2.10. Informa a el(la) Gerente(a) de Sistemas Informáticos sobre la falla del equipo y entrega copia del informe.

El(La) Gerente(a) de Sistemas Informáticos

9.2.11. Elabora memorándum sobre la falla del equipo y lo envía a el(la) Director(a) /Gerente(a) /Jefe(a) del área al cual pertenece el equipo.

9.2.12. Solicita a el (la) Coordinador(a) de Infraestructura Tecnológica la devolución del equipo al usuario encargado del activo.

El(La) Técnico(a) de Soporte de Sistemas Informáticos

9.2.13. Entrega el equipo con daño irreparable a la persona que lo tiene a cargo y documenta la falla en el formulario para traslado de activo fijo por reparación ().

El(La) Usuario(a)

9.2.14. Si el recurso informático presenta un daño irreparable procede a trasladar el activo hacia la Gerencia de Sistemas Informáticos.

El(La) Coordinador(a) de Infraestructura Tecnológica / El(la) Técnico(a) de Soporte de Sistemas Informáticos

9.2.15. Procede a preparar un equipo para sustituir el equipo dañado.

9.2.16. Coordina con el(la) encargado(a) de activo fijo la asignación del equipo.

9.2.17. Entrega el equipo al usuario, realiza pruebas de funcionamiento

El(La) Usuario(a)

9.2.18. Recibe recurso informático luego del mantenimiento correctivo y verifica su correcto funcionamiento, firma el formulario para traslado de activo fijo por reparación () y lo entrega a el(la) técnico(a) de soporte de sistemas informáticos.

9.2.19. En caso el equipo haya presentado falla irreparable, el (la) Usuario(a) recibe un recurso informático en sustitución del equipo que presentó la falla y verifica su correcto funcionamiento.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

El(La) Técnico(a) de Soporte de Sistemas Informáticos.

9.2.20. Archiva el formulario para traslado de activo fijo por reparación (FOGSI002) y registra en el Sistema de incidentes que la falla ha sido solventada y cierra la atención de la incidencia.

10. REGISTROS

Plan de Mantenimiento Preventivo de recurso informático.
Formulario para traslado de activo fijo por reparación.
Hoja de Mantenimiento Preventivo.
Lista de control de mantenimiento preventivo.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

11. ANEXOS:

Anexo 1. Prueba teórica

Defensoría del Consumidor

GOBIERNO DE EL SALVADOR

DEFENSORIA DEL CONSUMIDOR

Gerencia de Sistemas Informáticos

Fecha: _____

Nombre del estudiante: _____

Institución Educativa: _____

Nivel académico a la fecha: _____

PRUEBA DE CONOCIMIENTOS GENERALES PARA EL MANTENIMIENTO PREVENTIVO

NOTA: Esta prueba es de uso exclusivo de la Gerencia de Sistemas Informáticos de la Defensoría del Consumidor y se realiza con el fin de medir los conocimientos generales de los/las estudiantes. En ningún momento será publicada a terceros.

Prueba Teórica

1. [redacted]

2. [redacted]

3. [redacted]

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP"

4. [redacted]

5. [redacted]

6. [redacted]

7. [redacted]

8. [redacted]

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Anexo 2. Prueba práctica

Defensoría del Consumidor

GOBIERNO DE EL SALVADOR

Prueba Práctica

Será llenada por el Técnico de la Gerencia de Sistemas Informáticos.

1	[redacted]		
2			
3			
4			
5			
6			
7			
8			
9			
10			

Entrevista:

1. [redacted]
2.
3.
4.
5.
6.
7.
8.
9.
10.

OBSERVACIONES:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Defensoría del Consumidor

PROCEDIMIENTO PARA SOLICITUD INICIAL DE PROYECTOS Y REQUERIMIENTOS

(CÓDIGO:, VERSIÓN:)

Aprobado:

Presidente de la Defensoría del Consumidor

Fecha:

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP"

Elaboró:	Revisó:
Gerente de Sistemas Informáticos	Director de Administración Jefe de Planificación y Calidad

1. BASE LEGAL

Normas técnicas de control interno específicas de la Defensoría del Consumidor, Art. 70.
Reglamento para el uso y control de las tecnologías de información y comunicaciones en las entidades del sector público, Art. 14 y 15.

2. OBJETIVO

Establecer los lineamientos a seguir por parte de las diferentes unidades, gerencias y direcciones de la Defensoría del Consumidor (DC), para realizar la solicitud de un proyecto o requerimiento de desarrollo de software.

3. ALCANCE

El presente procedimiento aplica para toda unidad organizativa de la Defensoría del Consumidor, en lo referente a la solicitud de proyectos y requerimientos, ya sean, nuevos sistemas informáticos, agregar y/o modificar funciones de los sistemas existentes, generación de reportes, extracción y manipulación de datos de las bases de datos y cualquier otra actividad relacionada con los sistemas informáticos.

4. VIGENCIA

El presente documento entrará en vigencia ocho días hábiles posteriores a la aprobación por el (la) Presidente(a) de la Defensoría del Consumidor.

5. REFERENCIAS NORMATIVAS

"No aplica".

6. RESPONSABLE

Los responsables de la aplicación de este procedimiento son todas las jefaturas en cuyas unidades se realice una solicitud de desarrollo de proyectos o requerimientos de software, así mismo la Gerencia de Sistemas Informáticos será la responsable de velar que las unidades correspondientes cumplan con el procedimiento.

7. DEFINICIONES Y TERMINOLOGÍA

*Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP.

Desarrollo de software: Hace referencia a las actividades de análisis, diseño, programación, pruebas y puesta en producción de un programa o sistema informático.
Sistema informático: Herramienta de software que permite la automatización de uno o varios procedimientos de la unidad a la que pertenece.
Requerimiento: Solicitud de creación o modificación de una funcionalidad en un sistema informático nuevo o existente.
Grados de complejidad: Según el conjunto de características que posea un proyecto/requerimiento este puede ser catalogado en 3 niveles de complejidad, según se describe a continuación:

- **NIVEL I:** Requerimientos que involucran cambios menores y en un tiempo de ejecución entre 1 – 7 días hábiles, ejemplo: modificar un formulario y modificar un reporte.
- **NIVEL II:** Proyectos/requerimientos que involucran la creación de nuevas pantallas y reportes, corresponden a una actualización de un sistema existente, involucran un proceso de diseño de interfaces y cambios a nivel de base de datos. Requieren además de un proceso de levantamiento de requerimientos con el área (s) solicitante de 1 a 4 semanas y un plan de trabajo. Con una ejecución entre 1 a 8 semanas. Para un total máximo de 12 semanas.
- **NIVEL III:** Proyectos/requerimientos que involucran la creación de un nuevo sistema informático, creación de nuevos módulos, cambios de procesos a los sistemas existentes y creación/modificación de las estructuras de las bases de datos. Además, estos proyectos/requerimientos necesitan un estudio de factibilidad, proceso de levantamiento de requerimientos, diseño de interfaces, diseño de reportes y plan de trabajo. Con un tiempo de ejecución mayor a 12 semanas.

8. REQUISITOS

Formulario de *solicitud de proyectos y requerimientos* debidamente completada, según los lineamientos descritos en el *Manual del formato de Solicitud Inicial de Proyectos y Requerimientos*.

9. PASOS

Usuario(a) del área solicitante

9.1 Debe descargar el formulario de *solicitud de proyectos y requerimientos,* el cual se encuentra alojado en la plataforma SINCO.
9.2 Llenar todos los campos del formulario, según el tipo de solicitud y siguiendo los lineamientos del *Manual del formato de Solicitud Inicial de Proyectos y Requerimientos.*
9.3 Director(a), Jefe(a), Gerente(a) del área solicitante firma y sella la solicitud.
9.4 Se remite la *solicitud de proyectos y requerimientos* a la Gerencia de Sistemas Informáticos.

Gerente(a) de Sistemas Informáticos

9.5 Recibe la *solicitud de proyectos y requerimientos*.
9.6 Revisa la *solicitud de proyectos y requerimientos.*
9.7 Si existen observaciones en la *solicitud de proyectos y requerimientos,* se remite al área solicitante. En caso de no tener observaciones, se da el visto bueno a la solicitud.
9.8 Se remite la *solicitud de proyectos y requerimientos* a Presidencia de la Defensoría del Consumidor.
NOTA: Si el Gerente(a) de Sistemas Informáticos determina que la solicitud posee una complejidad de nivel I. Se podrá proceder a ejecutar la solicitud y al final del mes en curso se enviará un informe recopilatorio a Presidencia de la DC para para que apruebe los desarrollos ejecutados.

Presidencia de la Defensoría del Consumidor

9.9 Recibe la *solicitud de proyectos y requerimientos*.
9.10 Revisa la solicitud de proyectos y requerimientos.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

9.11 Si existen observaciones en la *solicitud de proyectos y requerimientos,* se remite al área solicitante. En caso de no tener observaciones, se da el visto bueno a la solicitud.

9.12 Remitir a la Gerencia de Sistemas Informáticos la *solicitud de proyectos y requerimientos* aprobada.

Gerente(a) de Sistemas Informáticos

9.13 Recibe la *solicitud de proyectos y requerimientos* aprobada por Presidencia de la Defensoría del Consumidor.

9.14 Convoca a Coordinador(a) de Desarrollo y/o Coordinador(a) de Infraestructura Tecnológica, para realizar un análisis preliminar y determinar el nivel de complejidad de la solicitud.

9.14.1 Si la Gerencia determina que el alcance posee una complejidad nivel II o nivel III:

9.14.1.1 Se convoca a una reunión preliminar con las áreas involucradas a fin de establecer el alcance.

9.14.1.2 Se realizará un estudio de viabilidad e informará a Jefatura que hace el requerimiento y Jefatura de la Dirección de Administración, para determinar su ejecución.

9.14.1.3 Si el proyecto es viable se procede conformar la Comisión responsable de la ejecución del proyecto, la cual será la encargada de realizar el plan de trabajo y velar por la ejecución del mismo, con el liderazgo de la unidad que realiza el requerimiento.

9.14.2 Si la Gerencia determina que el alcance en la solicitud posee una complejidad nivel I, se procede a realizar las modificaciones según lo descrito en la *solicitud de proyectos y requerimientos*.

10. REGISTROS

Solicitud Inicial de Proyectos y Requerimientos.

11. ANEXOS

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Manual del formato de Solicitud Inicial de Proyectos y Requerimientos.

Estructura del formato de solicitud

El documento está conformado por las siguientes partes:

1. Datos generales

Esta sección se utiliza para describir las generalidades del requerimiento/proyecto de software.

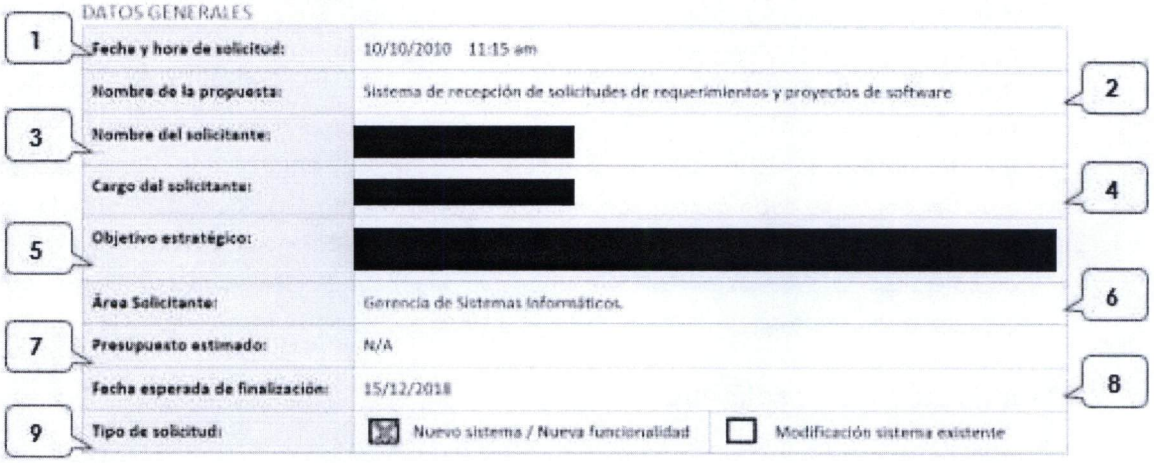


Ilustración 2 Sección - Datos generales

Donde:

1. **Fecha y hora** en que se realiza la solicitud, se deben colocar los valores correspondientes al momento de entrega de la solicitud a la GSI.
2. **Nombre de la propuesta**, el nombre que tiene la propuesta debe ser auto descriptivo y suficientemente claro para evitar ambigüedades, ejemplo: *Agregar un nuevo campo para registrar múltiples direcciones de notificación de un consumidor o proveedor.*
3. **Nombre del solicitante**, corresponde a la persona que realiza la solicitud, la persona que será responsable de brindar la información sobre el requerimiento/proyecto o quien delegará a la(s) persona(s) que brindarán la información y acompañamiento en el proceso. Pueden ser múltiples solicitantes en caso de que el requerimiento/proyecto este compartido con otra unidad.
4. **Cargo del solicitante**, el cargo que posee la o las personas que realizan la solicitud.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

5. **Objetivo estratégico,** en este apartado se debe colocar el objetivo (estratégico, POA u otros) al que pertenece este proyecto/requerimiento, en caso de que no persiga ninguno de estos objetivos se debe marcar como 'N/A'.
6. **Área solicitante,** Dirección, Unidad o Gerencia a la que pertenecen la o las personas solicitantes.
7. **Presupuesto estimado,** en caso de que el requerimiento/proyecto tenga un presupuesto asignado se debe colocar en este campo para efectos de la planificación y asignación de recursos. En caso de no poseer presupuesto se debe colocar 'N/A'.
8. **Fecha esperada de finalización,** en caso de que el requerimiento/proyecto tenga una fecha límite de implementación, se debe colocar en este campo. En caso de no poseer fecha límite se debe colocar 'N/A'.
9. **Tipo de solicitud,** se debe seleccionar el tipo de la solicitud, para ellos se cuenta con dos espacios donde se debe marcar con una **X** según sea el caso. Las opciones disponibles son **Nuevo sistema / Nueva funcionalidad,** la cual debe ser seleccionado cuando sean nuevas características a sistemas existentes o un nuevo sistema y **Modificación sistema existente** cuando se requieren cambios a funciones de un sistema existente.

2. Descripción de la solicitud

Esta sección se utiliza para detallar los objetivos y alcances del proyecto o requerimiento.

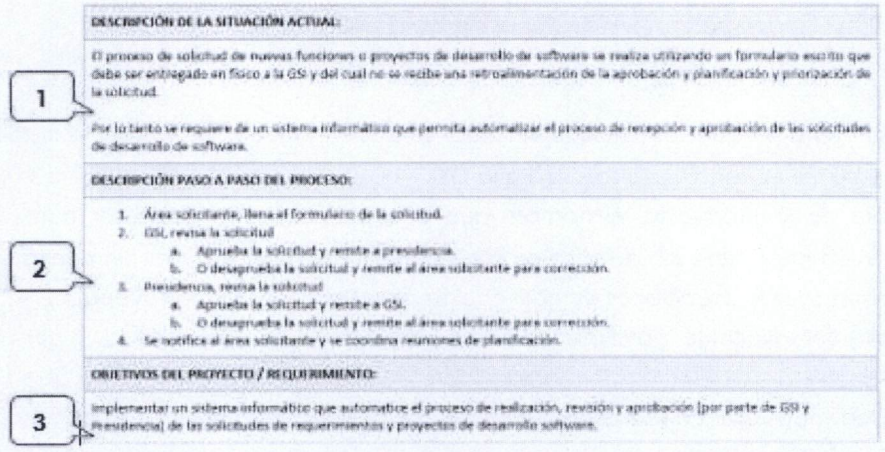


Ilustración 3 Sección – Descripción de la solicitud; parte I

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

Donde:

1. Se debe describir ampliamente la situación actual, los antecedentes que dan origen a la necesidad de este requerimiento o proyecto. En esta sección se pueden colocar imágenes, documentos anexos, capturas de pantalla y todo elemento que ayude a describir el punto.
2. Se debe detallar la serie de pasos que debe cumplir el requerimiento/proyecto solicitado, también se puede agregar un diagrama de procesos, flujograma, algoritmo, formulas, ecuaciones, etc.
3. Se debe describir de manera clara cuál es el objetivo que se pretende cumplir al realizar este proyecto/requerimiento.

RESULTADOS ESPERADOS (CRITERIOS DE ACEPTACIÓN): 4

1. Automatización del proceso.
2. Que los usuarios solicitantes, GSI y presidencia puedan realizar seguimiento de las solicitudes realizadas.
3. Recibir notificaciones por correo electrónico cuando una solicitud ha sido aprobada o rechazada.
4. Generar reportes de las solicitudes por unidad, por estado y por fecha.

SISTEMAS INVOLUCRADOS / SISTEMAS A MODIFICAR: 5

1. SINCO; se debe iniciar sesión con la base de usuarios de SINCO.

UNIDADES/GERENCIAS INVOLUCRADAS: 6

1. Unidades solicitantes
2. GSI
3. Presidencia

ROLES/PERFIL DEL USUARIO(S) FINALES QUE UTILIZARAN EL SISTEMA: 7

NOMBRE	CARGO	USUARIO DE SISTEMA
Solicitante, puede ser de cualquier unidad, gerencia o dirección.		
[redacted]	Gerente GSI	N/A
Presidente o delgado de presidencia		N/A

Ilustración 4 Sección – Descripción de la solicitud; parte II

Donde:

4. Se deben listar todos aquellos elementos que se esperan como resultado de implementar el proyecto/requerimiento. En esta sección se puede colocar imágenes, documentos anexos, capturas de pantalla y todo elemento que ayude a describir el punto.
5. Se deben listar todos los sistemas que se verán afectados o con los que interactuará el nuevo proyecto/requerimiento además de identificar los procesos, estados, roles, etc.

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

6. Se deben listar unidades, gerencias o direcciones que se verán impactadas con este proyecto requerimiento, esto con el fin de tomarlos en cuenta en el proceso de toma de requerimientos, capacitaciones y migración de datos (en caso lo requiera).
7. Se deben identificar las personas que utilizaran el nuevo sistema o funciones desarrolladas.

3. Aprobación área solicitante

En esta sección las personas listadas en **Nombre del solicitante** en la sección de datos generales, deben firmar de conformidad con lo que han manifestado en la solicitud, deben firmar todas las personas solicitantes.

APROBACIÓN AREA SOLICITANTE

En el presente documento están definidas el alcance, características y objetivos que debe cumplir el requerimiento/proyecto solicitado. Sin más que hacer constar firmamos en muestra de aceptación, aprobación y entera satisfacción.

Aprobado por	Cargo	Firma	Fecha

Ilustración 5 Sección - aprobación área solicitante

4. Visto Bueno de Gerencia de Sistemas Informáticos

La Gerencia de Sistemas Informáticos, será la encargada de revisar la solicitud y verificar que el alcance, objetivos y resultados esperados estén claramente definidos. La GSI podrá aprobar la solicitud firmando y sellando de conformidad para luego ser remitida a presidencia o podrá realizar observaciones a la unidad solicitante.

VISTO BUENO DE GERENCIA DE SISTEMAS INFORMÁTICOS

Nombre	Firma	Fecha

Sello GSI

Sello GSI

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

5. Aprobación de presidencia

Cuando la solicitud ha sido aprobada por la GSI, será remitida a presidencia para su aprobación definitiva, una vez aprobada la solicitud es remitida a la GSI. En caso de encontrar observaciones será remitida a la unidad solicitante.

Para de aprobar la solicitud, el Presidente de la DC deberá firmar y sellar la solicitud.

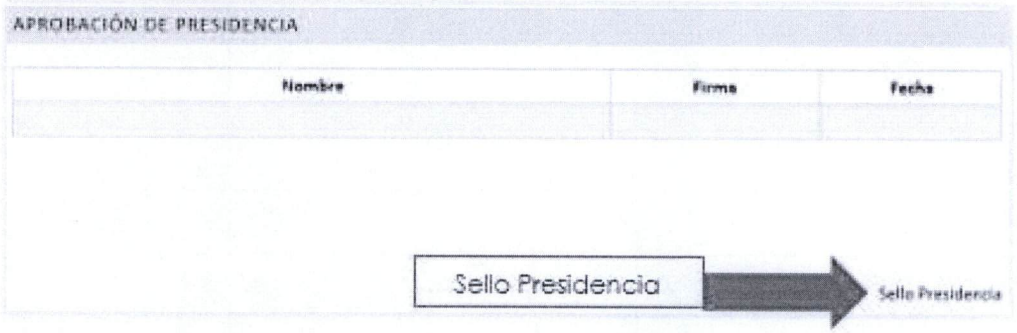


Ilustración 7 Sección - aprobación Gerencia de Presidencia

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."

HISTORIAL DEL DOCUMENTO

VERSIÓN	FECHA ELABORACIÓN / MODIFICACIÓN	DESCRIPCIÓN DE MODIFICACIÓN

"Sobre el presente documento se elaboró una versión pública, de conformidad al Artículo 30 de la Ley de Acceso a la Información Pública (LAIP), protegiendo los datos personales de las partes que intervinieron en el presente proceso; así como datos confidenciales, según lo establecido en el Artículo 6 letras "a", "f" y, 24 de la LAIP."