PROCEDIMIENTO
SISTEMAS Y REDES INFORMÁTICAS
P-TI-002

TABLA DE CONTENIDOS

Tabla Resumen Motivo de Revisiones del Procedimiento			
Motivo de los Cambios	**Fecha**	**Nº Rev.**	**Páginas**
Se Emite Documento	30.Ago.24	01	Todos

ELABORADO POR	**REVISADO POR**	**APROBADO POR**
Encargado(a) Soporte Informático Dirección TI	**Director de Tecnologías de la Información**	**Director de Tecnologías de la Información**

1. Objetivo

El objetivo de este procedimiento es establecer y estandarizar las acciones necesarias para mantener un nivel mínimo de calidad de servicio respecto a los sistemas y redes de la Fundación.

2. Alcance

Aplica al Dirección de Tecnología de la información como responsable y coordinador de la estructura informática de la fundación; y a los Programas que deben cumplir las normativas respecto a la utilización de sistemas y gestión de redes informáticas.

3. Referencias y Definiciones

3.1 Referencias

3.1.1 Política de Seguridad de la Información (**D-TI-001**).

3.2 Definiciones

3.2.1 **Política de Seguridad de la Información:** Documento que da el marco de referencia para la implementación del Sistema de Seguridad de la Información de la Fundación, basado en la Norma ISO 27001/2009.

3.2.2 **Procedimientos:** Documentos en los cuales se describe la secuencia de realización de las actividades técnicas y/o administrativas, y la interrelación de los diferentes Direcciones y/o Programas **para alcanzar un propósito especifico**, como, por ejemplo, la elaboración de documentos, la formulación de un Proyecto, etc. (quién o quiénes lo hacen, qué se hace, cómo se hace y cuándo se hace).

3.2.3 **Instructivos de Trabajo:** Documentos en los que se detallan las actividades específicas **para la realización de una actividad operativa**, como, por ejemplo, la creación de cuentas de correo, eliminación de accesos, solicitud de soporte, entre otros. (quién o quiénes lo hacen, qué se hace, cómo se hace y cuándo se hace).

3.2.4 **Formularios:** Documentos (plantillas) en los que se registran los resultados de las actividades declaradas en los procedimientos o instructivos de trabajo, los cuales forman parte de la evidencia objetiva requerida para demostrar que el sistema gestión de calidad cumple lo establecido en los citados documentos.

3.2.5 **Sistema Informático**: Sistema que permite almacenar y procesar información, compuesto por hardware, software y las personas que lo utilizan (ejemplos de sistemas informáticos son correo electrónico de la fundación, sistemas de gestión interna, intranet).

3.2.6 **Bienes informáticos**: Son todos aquellos elementos que forman el sistema en cuanto al hardware, ya sea la unidad central de procesos o sus periféricos (computador, escáner, impresora, monitor y otros).

3.2.7 **Red informática**: Conjunto de equipos informáticos conectados entre sí a través de dispositivos físicos para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

3.2.8 **Incidente de seguridad de la información**: se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la

operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información de la fundación.

4. Responsabilidades

4.1 Será responsabilidad del **Encargado de Soporte de TI**:

- Velar por el **correcto funcionamiento de los sistemas** informáticos de la fundación.
- Realizar **respaldos de los sistemas informáticos** de la fundación con una periodicidad pertinente para recuperación en caso de fallas minimizando la pérdida de información.
- Controlar que los sistemas informáticos estén disponibles, según su criticidad. Esto se logra a través de la generación de una estructura técnica que permita una buena **disponibilidad de servidores y servicios,** a través de sistemas físicos y/o virtuales.
- Dar **lineamientos respecto a la construcción de la red** de la fundación, controlando su distribución, tipos de enlaces, y protocolos que deben ser utilizados.
- Tomar las decisiones y acciones necesarias para realizar la **planificación de la estructura técnica de servidores** y redes de la fundación.
- Validar la **seguridad de acceso a los sistemas, servidores y redes**, a través de accesos restringidos de forma física y digital.
- Mantener **información actualizada de los enlaces de red de la fundación**, tanto a nivel central como en los programas.
- Mantener los servidores con los **parches de seguridad actualizados**, para sistemas operativos y sistemas implementados.

4.2 Será responsabilidad de los **Directores(as) Programas**:

- **Informar a nivel central** la estructura de red y accesos a sistemas desde el programa.
- **Seguir las indicaciones dadas por nivel central** respecto a los servicios que deben ser contratados para mantener una calidad de servicio aceptable que permita el acceso a los sistemas de la fundación.

5. Actividades

5.1 Revisión respaldo de sistemas informáticos

5.1.1 Todos los servidores de la fundación deben ser respaldados, sean estos físicos o virtuales, se manejen internamente o estén externalizados. Se debe validar en el caso de los servidores externalizados, en caso que el respaldo lo realice el proveedor, que entregue información respecto a la periodicidad y validación de los respaldos.

5.1.2 Los servidores deben ser respaldados dentro de lo posible con respaldos incrementales diarios automáticos y en un repositorio físico distinto ubicado en un lugar alejado respecto a la información real. Se debe proveer 2 tipos de respaldo:

- Respaldo incremental diario con 3 copias de la información.
- Respaldo incremental semanal.

5.1.3 Se debe revisar mensualmente que los respaldos se estén ejecutando correctamente, validando que todos los servidores se hayan respaldado y que no haya errores en los archivos respaldados o la comunicación. Para esto se dispone de un formulario con el listado total de servidores y los respaldos realizados correctamente (F-TI-005).

5.1.4 Para cada servidor respaldado se debe definir los pasos de recuperación ante desastres, respecto a la información que debe ser copiada y la configuración que debe tener el o los servidores.

5.1.5 Se recomienda revisar los respaldos realizados, para validar que puedan recuperar toda la información, a través de simulaciones de recuperación de la información y puesta en marcha de servidores.

5.2 Levantamiento y actualización de red informática

5.2.1 Se debe realizar un levantamiento de la red informática de la fundación, la cual debe ser actualizada cada 12 meses. Esta debe incluir las conexiones entre las oficinas centrales y los programas de la fundación, indicando como se conectan, tipo de enlace y servicios que tienen disponibles.

5.2.2 Para el levantamiento se dispone un formulario de registro de dependencias y enlaces (F-TI-006)

5.3 Revisión sistema de correos

5.3.1 Semanalmente se debe revisar el comportamiento del servidor de correos de la fundación, que corresponde a un servicio crítico para el trabajo diario del personal. Se debe validar lo siguiente:

- Espacio disponible en el servidor: validar que el servidor tenga espacio necesario para operar correctamente.
- Revisión de cuentas en tamaño crítico: las casillas llenas dejan de recibir o enviar correos, se debe indicar cuales necesitan que los correos sean descargados o aumentar su tamaño si corresponde.
- Reiniciar servidor de correos.
- Actualización de parches de seguridad.
- Revisión de filtros de spam.

5.4 Incidentes de seguridad

5.4.1 Cualquier incidente de seguridad de la información debe quedar registrado en un a través de un formulario (F-TI-007), en el cual se indicará cual fue el problema ocurrido, la fecha y quien lo reportó.

5.4.2 Una vez al mes se debe revisar los incidentes ocurridos e indicar las acciones a realizar para mitigar el riesgo, sean estas preventivas o correctivas, a través del mismo formulario de incidente de seguridad.

6. Registros

6.1. Registro de servidores y respaldos (**F-TI-005**)

6.2. Registro de dependencias y enlaces (**F-TI-006**)

6.3 Incidentes de seguridad de la información (**F-TI-007**)

7. Anexos

No Aplica