



V4

PROCEDIMIENTO

PROCESO: GESTIÓN DE LA INFORMACIÓN Y LA TECNOLOGÍA

PROCEDIMIENTO: SEGURIDAD DE LA INFORMACIÓN

VIGENCIA DESDE: 23/11/2018

CODIGO: 127-PRCGI-02

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
2	23/05/2017	Se realizan modificaciones a las actividades, organizandolas de tal manera que se ajusten al procedimiento como actualmente se realiza en la Oficina de Sistemas
3	30/08/2018	Se incluyó dentro del procedimiento el Formato de control de cambios y el listado maestro de cambios.
4	23/11/2018	Se realiza actualización del procedimiento, con el fin de alinearlo a las actualizaciones Manual de Gestión de Seguridad de la Información 127-MANGI-01 y de la Guía de Seguridad de la Información 127-GUIGI-01

OBJETIVO
Garantizar la confidencialidad, integridad y disponibilidad de la información, haciendo adecuado uso de las políticas de seguridad establecidas.

ALCANCE
Inicia con la identificación y análisis de las posibles riesgos y amenazas a las que está expuesta la información y termina con las acciones preventivas, detectivas y correctivas que salvaguarden la Confidencialidad, Integridad y Disponibilidad. Aplica a todos los procesos de la Entidad.

DEFINICIONES Y SIGLAS

DEFINICIONES:

- AMENAZA: Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño.
- BACKUP: Copia de los datos originales, total o parcial, que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.
- CONFIDENCIALIDAD: Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. A groso modo, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.
- DISPONIBILIDAD: Posibilidad de acceder a la información de la Entidad de manera activa, permanente, segura y confiable obteniendo aquello que se necesita.
- INTEGRIDAD: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.
- POLÍTICAS DE SEGURIDAD: Conjunto de buenas prácticas para el manejo de la información.
- RIESGO: Es todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas. Los riesgos más perjudiciales son a las tecnologías de información y comunicaciones. Tambien se define como el grado de exposición a la que nos encontramos ante la ocurrencia de un evento.
- SEGURIDAD INFORMÁTICA: Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

SIGLAS:

POLÍTICAS DE OPERACIÓN Y ASPECTOS GENERALES

1. Para el desarrollo de este procedimiento, se debe revisar la Guía para la Seguridad Informática del DADEP.
2. Las actividades que son punto de control, serán señaladas dentro del Flujoograma con la figura de cuadrado y la sigla P.C. dentro de ella.
3. Cuando en las actividades se presenten incumplimiento de requisitos de norma o de los clientes y/o usuarios, deberán implementarse el procedimiento denominado "Acciones correctivas, preventivas y de mejora".
4. Cuando dentro del procedimiento se incluyan acciones de divulgación o comunicación estas deberán realizarse en el marco del Plan de comunicaciones del Departamento y deberá tener en cuenta los procedimientos y protocolos establecidos

PRODUCTO O SERVICIO		
SALIDAS (Producto o Servicio)	DESCRIPCIÓN	CLIENTE
Información y documentos disponibles y protegidos.	Hace referencia a la posibilidad de acceder a la información de la Entidad de manera activa, permanente, segura y confiable obteniendo aquello que se necesita.	
Back-Up.	Copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida, riesgo o contingencia.	

NORMATIVIDAD Y/O DOCUMENTOS ASOCIADOS

- La normativa asociada al procedimiento se puede consultar en el siguiente vínculo: Normograma
- Los documentos asociados al procedimiento se pueden consultar en el siguiente vínculo: Listado Maestro de Documentos.
- Las disposiciones de almacenamiento y archivo se pueden consultar en el siguiente vínculo: Tablas de Retención Documental.

ACTIVIDAD	FLUJOGRAMA	DESCRIPCIÓN ACTIVIDAD	RESPONSABLE	FORMATO Y/O REGISTRO
		Inicio.		
1		Establecer y ajustar las Políticas de Seguridad de la Información del DADEP.	Profesional de planta y/o contratista encargado de la seguridad de la información	Guía de Seguridad de la Información 127-GUIGI-01
2		Revisar y aplicar las Políticas Informáticas de seguridad.	Profesional de planta y/o contratista encargado de la seguridad de la información	Guía de Seguridad de la Información 127-GUIGI-01
3		Hacer seguimiento periódico a las posibles amenazas a las que esta expuesta la información de la entidad.	Profesional de planta y/o contratista encargado de la seguridad de la información	Guía de Seguridad de la Información 127-GUIGI-01
		¿Se detectaron vulnerabilidades, amenazas o problemas que afecten la seguridad de la información? Si, Pasa a la actividad 4. No, Pasa a la actividad 3.	Profesional de planta y/o contratista encargado de la seguridad de la información	Guía de Seguridad de la Información 127-GUIGI-01
4		Identificar y analizar el tipo de vulnerabilidades, amenazas o problemas, de acuerdo a la Guía Seguridad de la Información del DADEP.	Profesional de planta y/o contratistas encargados de la seguridad de la información, infraestructura tecnológica y sistemas de información	Guía de Seguridad de la Información 127-GUIGI-01
5		Gestionar las vulnerabilidades, amenazas y problemas teniendo en cuenta a los lineamientos Guía Seguridad de la Información del DADEP. *El tiempo puede ser mayor dependiendo de la amenaza	Profesional de planta y/o contratistas encargados de la seguridad de la información, infraestructura tecnológica y sistemas de información	Guía de Seguridad de la Información 127-GUIGI-01
6		Realizar acciones de verificación, actualización o mejora al Sistema de Gestión de la Seguridad de la Información.	Profesional de planta y/o contratista encargado de la seguridad de la información	Plan de Seguridad y Privacidad de la Información
		Fin.		

AUTORIZACIÓN		
Elaboró:	Revisó:	Aprobó:
Carlos Rojas Villamil Contratista Oficina de Sistemas	Luis Fernando Arango Vargas Profesional Oficina Asesora de Planeación Isaías Sanchez Rivera Jefe Oficina Asesora de Planeación	Julio Alexander Hernandez Martinez Jefe Oficina de Sistemas