INSTITUTO DE PATRIMONIO Y CULTURA DE CARTAGENA DE INDIAS
IPCC

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI)
ARQUITECTURA EMPRESARIAL

Política de Backus

2025

INDICE DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVOS 3
2.1. GENERAL 3
3. ALCANCE Y ÁMBITO DE APLICACIÓN 3
4. NORMATIVIDAD 3
5. DEFINICIONES Y TÉRMINOS 4
6. DESCRIPCIÓN DE LA POLÍTICA 5
6.1. LINEAMIENTOS 6
6.1.1. IDENTIFICACIÓN DE INFORMACIÓN CRÍTICA 6
6.1.2. FRECUENCIA Y TIPO DE RESPALDO 6
6.1.3. PROTECCIÓN A LOS MEDIOS DE RESPALDO 6
6.1.4. PROTECCIÓN DE LA INFORMACIÓN EN MEDIOS DE RESPALDO 6
6.1.5. PERIODO DE EXISTENCIA DE LAS COPIAS DE RESPALDO Y SU EVENTUAL DESTRUCCIÓN 7
6.1.6. RESPALDO DE ESTACIONES DE TRABAJO 7
6.1.7. PRUEBAS DE RESTAURACIÓN DE LAS COPIAS DE RESPALDO 7
7. RESPONSABLES 7
8. INCUMPLIMIENTO 8
9. REFERENCIAS 8
CONTROL DE CAMBIOS 8

INTRODUCCIÓN

En el Instituto De Patrimonio y Cultura De Cartagena IPCC, la información es un activo valioso que sustenta nuestras operaciones diarias. Para proteger este activo y garantizar la continuidad del negocio, es fundamental contar con una estrategia sólida de copias de seguridad. Esta política define los procedimientos, responsabilidades y estándares técnicos necesarios para asegurar la protección de los datos de la organización ante eventos imprevistos como fallas del sistema, desastres naturales o ciberataques.

La pérdida de datos puede tener consecuencias devastadoras para cualquier organización, desde la interrupción de las operaciones hasta la pérdida de reputación y clientes. Esta política de copias de seguridad tiene como objetivo mitigar estos riesgos, estableciendo un marco sólido para la protección de la información crítica de la empresa.

Esta política de copias de seguridad se aplica a todos los sistemas informáticos y datos de Instituto De Patrimonio y Cultura De Cartagena IPCC, incluyendo servidores, estaciones de trabajo, aplicaciones y bases de datos. El objetivo principal es garantizar la disponibilidad de la información crítica en caso de pérdida o daño, minimizando el impacto en las operaciones y asegurando el cumplimiento de las regulaciones del estado.

OBJETIVOS

GENERAL

El objetivo de esta política es establecer las directrices y procedimientos para la creación, almacenamiento y restauración de copias de seguridad de los datos, con el fin de garantizar la disponibilidad y recuperación de la información crítica ante fallos del sistema, pérdida de datos o incidentes de seguridad.

Asegurar la generación de copias de respaldo de los datos y software del IPCC, asignando los roles, recursos y medios necesarios, estableciendo lineamientos de respaldo y almacenamiento de la información.

ALCANCE Y ÁMBITO DE APLICACIÓN

Esta política aplica a todos los sistemas, bases de datos, aplicaciones, archivos y recursos de la organización que contengan datos importantes. Incluye servidores, estaciones de trabajo, dispositivos móviles, y entornos en la nube. Que están bajo su administración; así mismo, garantizar que los terceros cumplan con los protocolos de backups definidos por el IPCC en el proceso contractual.

NORMATIVIDAD

NORMA	AÑO	DESCRIPCIÓN
Decreto 1727	2009	Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información
Decreto 235	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
Decreto 235	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
Decreto 235	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
NTC-ISO / IEC 27001:2013	2000	Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos
Ley 734	2002	Código Disciplinario Único

DEFINICIONES Y TÉRMINOS

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas...) que tenga valor para la Entidad.

Activos de Información: Es todo aquello que contiene, procesa, trate y/o manipule información valiosa para la Entidad y que son necesarios para que la Entidad funcione y cumpla con los objetivos establecidos para dicho fin.

Copia de respaldo o Backup: Es un duplicado de la información más importante, y se realiza para salvaguardar los documentos, archivos, fotos, bases de datos, configuraciones etc.

Naturaleza de la información: Análisis de lo que se va a copiar de nuestros sistemas. ¿Qué tipo de información se va a copiar? Completo (clonación o imagen), Sistema (registros, configuración), aplicaciones, bases de datos, documentos, etc. En función de la naturaleza de la información será necesario tomar decisiones como por ejemplo el tipo de software de backup a utilizar para que permita "copias en caliente".

Localización/Almacenamiento: En función de la situación de las copias estas podrían ser locales si los soportes se almacenan en las mismas instalaciones en las que se encuentra el sistema de información, remotas si se almacenan en un pabellón diferente, y externas si son realizadas por internet y almacenadas en servidores externos a la facultad. Los almacenamientos locales deberían contar con la máxima seguridad física por ejemplo mediante el uso de armarios ignífugos bajo llave y en las correctas condiciones ambientales.

Programación: La copia de respaldo se puede hacer de forma manual o automatizada y se debe tener en cuenta especialmente la hora elegida para hacerlas, prefiriendo las de menor actividad para reducir molestias a los usuarios (ya que no deberían estar trabajando mientras se hacen las copias). Ej. Horario nocturno.

Propietario de Activo de Información: Es el nombre del responsable de la producción de la información (propietario): Que corresponde al nombre del área, dependencia o unidad interna, o al nombre de la entidad externa que creó la información. Es el responsable del activo, quien debe velar por el cumplimiento de los requerimientos establecidos frente a las propiedades de disponibilidad, confidencialidad e integridad.

Tipo de Backup: En función de la cantidad de información a copiar, el backup puede ser completo (toda), incremental (sólo se copian los ficheros modificados o creados desde la última copia incremental) o diferencial (copia los ficheros modificados desde la última copia completa). La incremental necesita menos espacio, pero es más complicada de restaurar que la diferencial.

Software: La herramienta utilizada para realizar las copias debe soportar las características que se hayan planificado en función de las necesidades. Las copias se pueden programar con tareas mediante scripts de línea de comandos, o con un software específico (gratuito o invertir en sistemas de copias comerciales).

Soporte: Es el objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos. Se debe elegir el tipo de soporte de almacenamiento que mejor se adapte a las necesidades particulares del sistema en cuestión.

Volumen de información: Disponer de una estimación de la cantidad de datos a copiar. Esto será necesario para tener en cuenta por ejemplo que estrategia de copias utilizar, el tipo de soportes para realizar las copias o incluso estimar el tiempo necesario para realizar la copia.

DESCRIPCIÓN DE LA POLÍTICA

El IPCC considera que toda la información de sus sistemas informáticos críticos en producción debe ser protegida de posibles daños, por lo que debe ser respaldada con cierta frecuencia, para asegurar el proceso de recuperación.

Bajo esta premisa, la división administrativa y financiera y la oficina de Sistemas deberá considerar soluciones de respaldo para equipos de escritorio, servidores, sistemas de información y aplicaciones (códigos fuentes, bases de datos, etc.) que se consideren críticos para la Entidad. Igualmente, garantizar la disponibilidad de infraestructura adecuada de respaldo y asegurar su disponibilidad cuando sea requerida la copia, incluso después de un desastre o falla de un dispositivo.

Para los sistemas de información que no están bajo la administración la división administrativa y financiera y la oficina de Sistemas, ésta debe velar y validar que el tercero encargado cumpla con la presente política.

Información que NO es relevante para la Entidad y que resida en los servidores, sistemas de información y equipos de escritorio del IPCC, NO SERÁ respaldada. La importancia de realizar la copia de seguridad de la información la deberá informar el Jefe de Área o encargado de cada procedimiento en la matriz de activos de información.

Cada respaldo que se realice, manual o automático, deberá quedar registrado en los LOG de los servidores, o sistemas de información.

En las situaciones donde el activo de información a respaldar está categorizado como público clasificado o público reservado, se deberán ejecutar copias de respaldo cifradas.

LINEAMIENTOS

IDENTIFICACIÓN DE INFORMACIÓN CRÍTICA

El Jefe de Área o responsable de la información de cada procedimiento, será el responsable de identificar y conservar actualizados los activos de información.

El respaldo de la información de los sistemas integrados relacionado con activos compartidos debe ser solicitado por cada uno de los jefes de área que tienen responsabilidad sobre ellos.

FRECUENCIA Y TIPO DE RESPALDO.

El IPCC con el apoyo de sus encargados, deberá definir los tipos de copias a ejecutar para cada Sistema de Información.

Para cada copia de respaldo, se deberá considerar la frecuencia, los medios de almacenamiento, tipo de contenido, tiempo de almacenamiento y borrado de esta información.

La periodicidad con que se realizarán los respaldos de los computadores personales o estaciones de trabajo de la Entidad deberá ser mínimo de 1 respaldo anual, esta información es la que cada persona envía a la unidad Z y es responsabilidad de cada colaborador.

Todas las áreas que generan información deberán definir la frecuencia del respaldo de esta e informarle a la oficina de Sistemas, esta información se debe diligenciar en la matriz de activos de información.

PROTECCIÓN A LOS MEDIOS DE RESPALDO

Los medios de respaldo que contienen información deben tener una custodia que garanticen la protección adecuada de los datos allí almacenados, de forma que cumplan con los requisitos para ser puestos en funcionamiento en cualquier momento que sea requerido, además se deberá tener las copias de seguridad en un lugar secundario para mitigar riesgos en caso de un evento inesperado dentro de los sitios donde se generan las copias de respaldo.

Ante un cambio tecnológico que se produzca que pueda generar obsolescencia tecnológica, deben generarse las acciones necesarias de resguardo de la información de los medios de respaldo.

PROTECCIÓN DE LA INFORMACIÓN EN MEDIOS DE RESPALDO.

Deberán existir registros documentados de las copias de respaldo y del restablecimiento de estas. El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado.

Toda información crítica grabada en medios de respaldo que son almacenados fuera de la Entidad deberá ser trasladada con los elementos de seguridad adecuados, como por ejemplo el uso de controles criptográficos.

PERIODO DE EXISTENCIA DE LAS COPIAS DE RESPALDO Y SU EVENTUAL DESTRUCCIÓN

Cada Jefe de Área deberá determinar el período de conservación del respaldo de la información crítica de sus procesos, teniendo en cuenta los requisitos de conservación de las tablas de retención documental, la normativa legal vigente, el uso eficiente del espacio físico y los medios de almacenamiento disponibles.

RESPALDO DE ESTACIONES DE TRABAJO

La Oficina de Sistemas deberá considerar, dentro de sus recursos asignados, soluciones de respaldo para equipos de escritorio. Siendo los usuarios de la Entidad los responsables de alojar la información propia de su objeto contractual que necesita ser respaldada en los lugares establecidos para ello. No se respaldará información personal del usuario ya que en los computadores suministrados por el IPCC no está autorizado el almacenamiento de este tipo de información.

Se deberán utilizar los medios que la Oficina de Sistemas disponga para realizar las copias de respaldo.

La Oficina de Sistemas deberá asegurarse de que la información del objeto contractual del personal de la Entidad sea salvaguardada de forma satisfactoria.

PRUEBAS DE RESTAURACIÓN DE LAS COPIAS DE RESPALDO

La ejecución de las pruebas de restauración de las copias de respaldo deberá asegurar la recuperación de copias de datos, y garantizar la integridad de los datos que contienen.

Se deberán realizar pruebas respecto a la restauración de las copias de respaldo en forma controlada y en un ambiente seguro que contenga los mismos niveles de seguridad del ambiente original, de forma rotativa y con una periodicidad de mínimo 1 vez por año.

RESPONSABLES

Equipo de Seguridad de la Información:

- Velar por el cumplimiento de la presente política.

División Administrativa y financiera y Oficina de Sistemas:

- Designar el personal idóneo para definir y gestionar el estándar de respaldo de los servidores y equipos de hardware de la Entidad.
- Coordinar, ejecutar y velar por la realización de las copias de respaldo y restauración de estas, utilizando las herramientas pertinentes para tales efectos y validar que la actividad se realice correctamente.
- Mantener un inventario de los activos de información sobre los que se realizan copias de respaldo.
- Realizar pruebas periódicas de recuperación de información a partir de las copias de respaldo.

Áreas que Administran Sistemas de Información:

- El Jefe de Área o encargado mediante acto administrativo, podrá solicitar respaldos o restauración de las copias, según la necesidad que se requiera.

Todos:

- Dar cumplimiento a esta política.

INCUMPLIMIENTO

El incumplimiento de la Política de Backup de la Entidad podrá constituir falta disciplinaria y será sancionada en el marco del Código Disciplinario Único – Ley 734 de 2002.

REFERENCIAS

Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información – 2016.

International Organization for Standardization, ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems.

CONTROL DE CAMBIOS

Nº. VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	APROBADO POR