CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **"uso interno".**
El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.
No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrado en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. OBJETIVO

Fijar los lineamientos generales para la generación de respaldos de información (Backup) teniendo la posibilidad de recuperar la información de las bases de datos, File System y máquinas virtuales en ambientes de Producción, Preproducción, Pruebas y Desarrollo, además de correos electrónicos de ser necesario, previniendo la pérdida de información y asegurar el resguardo de los datos.

2. ALCANCE

El alcance de la presente política cubre el proceso de Backup de la información de los sistemas de información de Colombia, los cuales se encuentran alojados en los servidores del Datacenter Triara y en las nubes públicas de Azure y GCP.

3. DEFINICIONES

- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.
- **Información:** Datos relacionados que tienen significado para la organización. Además, es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.
- **Activo de Información:** Toda la información y el conjunto de elementos y medios que la soportan en su procesamiento y almacenamiento.
- **Backups: (Copia de seguridad):** Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo, como ser discos duros (D2D), CDs, DVDs o cintas magnéticas).

4. CONTENIDO

La alta Gerencia, la Gerencia, Subgerencia, Director y Administradores de Sistemas, son responsables de la implementación y cumplimiento de la política de copias de seguridad de la información.

La política de copias de seguridad de la información es de aplicación obligatoria para Ingenieros de sistemas cuyo rol esté asignado.

RESPONSABILIDADES DEL ADMINISTRADOR DE BACKUP

1. Configurar en las herramientas de respaldos cuando se requieran nuevas integraciones.
2. Monitorear que los trabajos de respaldos se ejecuten de forma correcta conforme a la definición de la política.
3. Escalar las fallas sobre los respaldos con los Administradores de Sistemas y/o Base de datos, según el caso.
4. Escalar con soporte local y/o el proveedor del Software de la herramienta las fallas presentadas sobre estas.
5. Actualizar el inventario de cintas.
6. Solicitar el traslado de cintas del Datacenter a las instalaciones del proveedor de custodia externa.
7. Solicitar el traslado de cintas del proveedor de custodia hacia el Datacenter.
8. Llevar el registro en la bitácora de eventos cuando se presente una afectación crítica.
9. Informar al Director y/o Gerente del área el estado de la capacidad.
10. Informar al Director y/o Gerente del área anomalías sobre la infraestructura de respaldos que pongan en riesgo la operación de esta.

TIPOS DE BACKUP

La presente política establece los siguientes tipos de backup.

- **Full:** Para todos los trabajos de backup semanales, quincenales, mensuales, anuales y respaldo de Logs de las bases de datos, servicios web y filesystem de servidores físicos y virtuales (VMware).
- **Full anual:** Se toma el último backup full mensual del año (diciembre).
- **Incremental:** Para los trabajos de backup diarios a nivel de filesystem y SQL Server.
- **Snapshots:** Para los backups de la infraestructura virtual por Veeam Backup & Replication.
- **Full Synthetic:** fin de semana.

- **Incremental:** Todos los días.

FRECUENCIA

Hace referencia a la periodicidad con que se ejecutan los trabajos de backup, el establecimiento de esta frecuencia depende del ambiente y la criticidad del elemento que se esté respaldando y es especificada en el esquema general de backups (Hoja de cálculo de Google Sheets “Keralty. Política / Bitácora de Backups Keralty”).

RETENCIÓN

La retención de los Backups, son establecidos para determinar el tiempo en que el backup tomado debe estar en custodia, sin importar bajo qué medio está alojado el backup.
La retención de cada una de las políticas de backup, se evidencian en el esquema general de backups (Hoja de cálculo de Google Sheets “Keralty. Política / Bitácora de Backups Keralty”).
Respondiendo a la Resolución 839 de 2017 para establecer el manejo, custodia, tiempo de retención, conservación y disposición final de los expedientes de las historias clínicas y el Decreto 1072 de 2015, en su artículo 2.2.4.6.13 para la conservación de documentos, se establece una retención de ***30 años sobre medio magnético.***

DISPOSICIÓN FINAL DE BACKUPS

En el momento en que se cumpla el periodo de retención de backups, se realizará la eliminación segura de la información del medio magnético; para tal efecto se generará un acta en donde conste la eliminación de toda información.

HERRAMIENTAS DE RESPALDO

Keralty cuenta con dos (2) herramientas de respaldo, teniendo la posibilidad de generar y alojar copias de seguridad tanto en disco como en cinta.

- Data protector.

  Aplicación de copias de seguridad y recuperación de datos para diversos entornos físicos, configurada en un Cell Manager's, Data protector en la última versión estable, la cual es utilizada para backup on-line a Disco o Cinta, Base de Datos, Oracle y SQL Server, y Granularidad de Servers, Sistemas Operativos, Aplicaciones y Fileservers por filesystem.

- Veeam Backup & Replication.
  Aplicación de copias de seguridad en su última versión estable, desarrollada para entornos virtuales basados en los hipervisores VMware vSphere y Microsoft Hyper-V., para backup y replicación de servidores mediante snapshots en la infraestructura virtual.

Adicionalmente, se cuenta con el servicio de generación de backups de la nube de Azure.

ACTUALIZACIÓN DE HERRAMIENTAS

Se realiza actualización del Software de las soluciones de respaldos a la última versión estable liberada por el fabricante, para obtener mejoras funcionales, mitigar vulnerabilidades y corregir bugs. También por recomendación del fabricante sea por identificación de vulnerabilidad.
Igualmente, cuando se realice alguna actualización en el S.O de los clientes y esta versión requiera en su matriz de compatibilidad una versión superior del Software y esta esté disponible.

ALMACENAMIENTO DE RESPALDOS

Para la ejecución de los trabajos de respaldo, se cuenta con dos medios de almacenamiento: Disco y Cintas.

- **Disco HPE StoreOnce 5200:** Almacenamiento de discos, las cuales están destinadas a contener la totalidad de ejecuciones de backup correspondientes a File System, ARC logs de Oracle, Transaccionales de SQL Server y snapshot de máquinas virtuales.
- **Disco HPE Apollo A4200:** Almacenamiento de discos, las cuales están destinadas a contener la totalidad de ejecuciones de backup correspondientes a File System, ARC logs de Oracle, Transaccionales de SQL Server y snapshot de máquinas virtuales.
- **Cintas LTO:** utilizadas para realizar el procedimiento de backup mensuales de las bases de datos, File System y respaldos históricos.
- **Almacenamiento en Nube Azure:** Se cuenta con almacenamiento suministrado por la nube pública de Microsoft para la aplicación de los backups según la demanda de los mismos.
- **Almacenamiento en Nube GCP:** Se cuenta con almacenamiento suministrado por la nube pública de Google Cloud Plataform para la aplicación de los backups según la demanda de los mismos.

ROTULACIÓN DE MEDIOS

La rotulación de los cartuchos de backup son usados para la identificación de las cintas de respaldo, esta rotulación debe realizarse empleando los rótulos manufacturados por Hewlett Packard, según las referencias liberadas por el fabricante. Ej: Q2011A, la secuencia de estos depende de los datos de locación y otros, representando el registro del cartucho en el sistema de control de inventario de cintas, uniéndose al registro de cada cartucho, obteniendo el rotulo que lo identifica como registro en la base de datos de la empresa de custodia de medios contratada.

CUSTODIA MEDIOS MAGNÉTICOS

Keralty cuenta el servicio de custodia de medios con la entidad Iron Mountain, cuando se requiere él envió se gestiona mediante el envío de correo electrónico a las cuentas dispuestas por la entidad para programar el traslado: recogida, préstamo y devolución de medios magnéticos.

RESGUARDO DE MEDIOS

La organización tiene contrato de:

- Servicio de custodia de medios y manos remotas con Claro S.A para la custodia de las cintas que se generan en el CellManager de Dataprotector y Consola de Veeam alojados en las librerías en Triara - Cuatro Casilleros de 13 slots – Casilleros 49, 50, 51 y 52. (Cintas que se trasladan a **Iron Mountain** cuando terminan los trabajos de Backup mensuales).
- Servicio de custodia de medios con **Iron Mountain** para la custodia de las cintas que se generan en los CellManager de Dataprotector y Consola de Veeam, de los respaldos mensuales, históricos o cualquier medio magnético del cual se requiere tener bajo altos estándares de seguridad.

MONITOREO

El monitoreo de los backups, tiene como objetivo asegurar la generación de los respaldos de seguridad. Las actividades están determinadas principalmente por las siguientes actividades.

- Monitorear la solución de backup.
- Relanzar los backup fallidos y escalar anomalías que afecten la correcta ejecución de los respaldos.

RESTAURACIONES

Las restauraciones de los backups serán controladas, en donde es necesario generar un requerimiento a través de la mesa de ayuda (MAS). Sobre dicho requerimiento se debe indicar los datos del backup para realizar la restauración.

A continuación, los datos mínimos para la solicitud de restauración.

- File System: fecha, servidor, ruta, carpeta y/o archivo
- Base de datos: fecha, servidor y base de datos
- Snapshot: fecha y servidor.

Para todas las restauraciones se debe indicar si la información se sobre escribe o no.

GENERALIDAD PARA BACKUPS SEGÚN AMBIENTES

BACKUP PARA AMBIENTE DE PRODUCCIÓN

Oracle

Se tienen configuradas con Full backup semanal y mensual de la base de datos y respaldo de archive logs full cuatro veces al día.

SQL Server

Se tienen configuradas con Full backup semanal y mensual de la base de datos y respaldo de logs transaccionales cada 15 minutos.

File System

Se tienen configuradas con Full backup semanal y mensual de file system e incrementales diarios de los servidores que son repositorios con información crítica solicitada para ser respaldada.

File System logs (opt y var)

Se tiene configurada un backup full semanal y un diario incremental de las rutas /opt y /var de los servidores de Aplicación críticos del negocio solicitando en respaldo.

Snapshot

Se realiza imagen de los servidores de criticidad alta, media y baja, los trabajos están agrupados por Aplicación de acuerdo a las maquinas que hacer parte de esta.

BACKUP PARA AMBIENTE DE PRE-PRODUCCIÓN

Respaldo de la metadata de cada base de datos con export el cual debe quedar en una ruta definida, con el objetivo de recuperación de claves configuradas, evitando afectación de pruebas durante una actualización de ambiente. (Cuando se hacen duplicado a cargo de Base de Datos).

Para los ambientes de Pre-producción, no se realiza toma de backups de toda la base de datos.

BACKUP PARA AMBIENTE DE PRUEBAS

Respaldo a demanda, teniendo en cuenta que NO se ejecuta backup sobre ninguna base de datos.

BACKUP PARA AMBIENTE DE DESARROLLO

Dado que el ambiente de desarrollo genera cambios constantes sobre la base de datos y/o servidores. A continuación, se evidencian las características de los backups para el ambiente de desarrollo.

- Diariamente se genera full export del 90% de las bases de datos en una ruta definida.
- Se respalda la información de la ruta diariamente con retención semanal y mensual con retención de 1 mes.
- Para las bases de datos de más de 30G se exporta la metadata que también queda en la ruta definida.
- El detalle del esquema de estas plataformas se puede observar en las tablas al finalizar este documento.

BACKUP CORREO ELECTRÓNICO

Este servicio utiliza la funcionalidad de Spanning Backup, una herramienta en línea que permite crear copias de seguridad de G Suite. Las copias se realizan a demanda, abarcando correos, Google Drive, contactos, sitios, entre otros. El acceso a esta herramienta está restringido a un número limitado de usuarios, principalmente de alto nivel, como vicegerencias y cuentas antiguas que ya contaban con este tipo de licenciamiento.

BACKUP NUBE

Este servicio es prestado por el proveedor del servicio en la Nube, bajo la política suministrada por el fabricante, el administrador o proveedor es responsable de la configuración, monitoreo y gestión. Igualmente es responsable de escalar cualquier novedad presentada sobre los backups y herramientas de respaldo.

INDICADORES

Se ha establecido que, para el aseguramiento de los backups, es necesario contar con dos (2) indicadores, siendo los siguientes:

Índice de backups exitosos

El indicador se obtiene de la medición de los backup exitosos sobre el total de los backups establecidos en la Política de backups de la organización (Keralty. Política / Bitácora de Backups Keralty), permitiendo tener una visión del estado de la ejecución de las políticas de respaldo establecidas.

Periodicidad: Mensual
Métrica: El cálculo del indicador se realiza teniendo presente la formula en relación:

$$\left(\frac{Total\ backups\ exitosos\ (Mes)}{Total\ backups\ programados\ según\ Política\ (Mes)}\right) * 100$$

Índice de restauración de backups exitosos

El indicador se obtiene de la medición de los backup exitosos sobre el total de los backups programados cada mes que debe ser mínimo de una (1) restauración por mes, para un total de mínimo doce (12) al año. Con lo anterior, se busca el aseguramiento de:

- Pruebas de proceso de restauración
- Pruebas de la generación de los backups
- Consistencia en datos respaldados

Periodicidad: Mensual

Métrica: El cálculo del indicador se realiza teniendo presente la formula en relación:

$$Índice\ de\ restauración = \left(\frac{Restauraciones\ exitosas\ (Mes)}{Restauraciones\ programadas\ (Mes)}\right) * 100$$

5. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
30/05/2014	Actualización	2
27/01/2015	Actualización	3
18/04/2017	Actualización	4
03/08/2017	Actualización	5
28/10/2020	Actualización Medios (StoreOnce)	6
11/05/2021	Actualización Política Oracle EBS	7
25/08/2021	Actualización Política Oracle y SQL Server	8
28/09/2022	Actualización Política y formato	9
11/12/2022	Actualización de Política	10
01/02/2023	Actualización de Política e inclusión de indicadores	11
09/08/2023	Actualización de retención de datos e inclusión de disposición de backups que cumplen periodo de retención	12
14/05/2024	El documento se revisa en el marco de la actualización del SGSI año 2024, se valida con el responsable del documento quien nos informa que a la fecha no existe ningún cambio en el contenido de este, se realiza inclusión de la sigla del país y la compañía en el código del documento	12.1
09/10/2024	Se actualiza documento, se retira las versiones de las cintas que se utilizan, se agregan información de almacenamiento en on-premise como en nube, se modifica información del backup de correo electrónico	13

Tabla 1 Control de cambios

6. FLUJO DE APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ
Nombre: Equipo Gerencia Corporativa de Tecnología Fecha: 09/10/2023	Nombre: Luisa Castaño Área/Proceso: Dirección Operaciones y Comunicaciones de TI Fecha: 09/10/2024	Nombre: Alejandro Ramírez Área/Proceso: Gerencia Corporativa de Seguridad Fecha: 09/10/2024 Nombre: Mauricio Forero Área/Proceso: Gerencia Corporativa de Soluciones Transversales Fecha: 09/10/2024 Nombre: Luisa Trujillo Área/Proceso: Gerencia Corporativa de Soluciones de Aseguramiento y Asistencial Fecha: 09/10/2024 Nombre: Karen Rincón Área/Proceso: Gerencia Corporativa de Salud Digital Fecha: 09/10/2024 Nombre: Adrián Esquinas Área/Proceso: Gerencia Datos y Analítica Fecha: 09/10/2024 Nombre: Javier Galván Área/Proceso: Gerencia Corporativa de Tecnología Fecha: 09/10/2024

Tabla 2 Flujo de Aprobación

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.