**Plan de Respaldo de Datos y Aplicaciones**

**PRESENTADO POR:   
JORGE ALBERTO HURTADO CORTÉS   
ANDRÉS FELIPE BABATIVA BETANCOURT   
DIEGO ANDRÉS SERNA PARUMA   
FRANCHESKA LOZANO HIDALGO**

**FICHA 2141041**

**SERVICIO NACIONAL DE APRENDIZAJE (SENA)   
CENTRO DE ELECTRICIDAD, ELECTRÓNICA Y TELECOMUNICACIONES   
BOGOTÁ D.C., SEPTIEMBRE 2021**

**Contenido**

Introducción ………..……………………………………………………………………………………… 3

¿Qué es el Plan de Respaldo de Datos y Aplicaciones? ……………………………….. 4

¿Por qué es importante el Plan de Respaldo de Datos y Aplicaciones? ……….. 4

Sobre el Plan de Respaldo de Datos y Aplicaciones ..…………………………………… 4

Implementación del backup ……………………………………..........………………………… 5

Identificación de vulnerabilidades ………………………………………………………..……. 5

Hora para realizar respaldos ……………………………………………………………………... 6

Realización del backup ………………………………………………………………………………. 6

Conclusiones ………………………………………………………………………………...………….. 6

**Introducción**

Este documento se presenta con el fin de contar con un plan de respaldo de datos y aplicaciones el cual demuestra la investigación que el equipo Weeklyst realizó para adecuar un proceso de respaldo eficiente para estimular las buenas prácticas y un correcto funcionamiento al momento de respaldar el proyecto que se realiza.

**¿Qué es el Plan de Respaldo de Datos y Aplicaciones?**

El Plan de Respaldo de Datos y Aplicaciones es un protocolo que establece una serie de pasos acordados por los desarrolladores o el equipo encargado de resguardar la información de un proyecto de desarrollo constituyendo un proceso que garantice un correcto y eficiente respaldo de la información.

**¿Por qué es importante el Plan de Respaldo de Datos y Aplicaciones?**

Es importante establecer este proceso desde un inicio para garantizar que todos los datos y la información de la aplicación cuentan con un respaldo que se realiza regularmente según esté definido en el plan de respaldo.

**Sobre el Plan de Respaldo de Datos y Aplicaciones**

Weeklyst está manejando repositorios en la plataforma GitHub, no está automatizado el proceso pero se actualiza el repositorio de manera manual e inmediata desde el editor de código Atom o el framwork utilizado cada vez que se realiza un cambio en la base de datos o en la aplicación web.

****

**1) Implementación del backup**

El respaldo de datos debe ser estudiado y analizado para tener el mínimo margen de error posible.  
Para implementar un backup es necesario conocer los servidores disponibles, la seguridad que brindan y la seguridad adicional que se le puede practicar a la base de datos y las aplicaciones.

**2) Identificación de vulnerabilidades**

Se busca analizar el proceso con el que se hacen los respaldos actualmente para identificar cualquier vulnerabilidad posible y hallar una solución óptima al problema que se pueda presentar.  
Para esto se tienen diferentes aspectos en cuenta, como lo son el saber quiénes pueden realizar un backup, quiénes pueden solicitar la información del buckup, si existe algún sistema de encriptación, etc.

Se deberá documentar cada actualización a los respaldos de datos, con el fin de identificar anomalías y tener un seguimiento concreto del backup.

En la documentación del proceso se tendrá en cuenta si hay amenazas; si se presenta vulnerabilidad física, de hardward, de software o humana.

**3) Hora para realizar respaldos**

Se debe hacer un estudio de tráfico de red en los servidores escogidos para almacenar la información, basado en eso se puede definir una hora que se cumpla cada día para mantener asegurada cada actualización realizada en el proyecto.

Se puede definir una hora específica para cada parte del proyecto, como lo son las interfaces gráficas, el back-end y la base de datos, puede realizarse un backup en horas determinadas para cada punto.

**4) Realización del backup**

Weeklyst se encuentra haciendo uso de GitHub para asegurar las copias de seguridad del proyecto, se tiene una carpeta en los equipos de cada desarrollador que contiene el proyecto completo, dicha carpeta está asociada a la herramienta Git para poder respaldar la información en cada actualización que realicen los desarrolladores involucrados.