

Arquitectura y Seguridad





Contenido

USUARIOS Y CLAVES DE ACCESO 7
1. Herramientas y manejo de usuarios 8
2. Acceso a los recursos 8
3. Llaves de configuración 9
ARQUITECTURA INTERNA DE LA SOLUCIÓN 10
1. Alcance 10
2. Generalidades 10
3. Diagrama General de la Arquitectura de la solución 10
4. Monitoreo Logs y Alertas 15
5. Mecanismos de Seguridad 15
6. Escalabilidad 16
6.1. Automática 17
6.2. Manual 17
7. Acuerdos de servicio - SLA 18
7.1. Monitoreo de los acuerdos de servicio - SLA 19
8. Alta disponibilidad y hot swap 20
ARQUITECTURA DE LOS METODOS DE MARCAJE 21
1. GeoVictoria USB 21
2. GeoVictoria BOX 25
2.1. Arquitectura 26
2.2. Disponibilidad del Servicio 26
2.3. Seguridad 28
3. GeoVictoria APP 28
3.1. Arquitectura 29
3.2. Lenguaje y entornos 30
3.3. Comunicación 30
3.4. Disponibilidad del servicio 31
3.5. Seguridad 33
3.6. Monitoreo y Alertas 42
4. GeoVictoria Call 43
4.1. Arquitectura 43
4.2. Disponibilidad del Servicio 44
4.3. Seguridad 45
ECOSISTEMA DE BASE DE DATOS 46

1. Ambiente 46
2. Tipos de base de datos y usos 48
2.1. Bases de datos relacionales 48
2.2. Bases no relacionales 49
3. Seguridad 49
3.1. Encriptación 49
3.2. Nivel de acceso 51
3.3. Roles 51
3.4. Usuarios 52
3.5. Acceso a la información 53
4. Redundancia de datos 53
4.1. Contenedor de archivos 53
4.2. Base de datos 54
5. Proceso de recuperación de datos 56
6. Tabla de riesgos 57
PROCESO DE DESARROLLO Y GESTIÓN DEL CAMBIO 60
1. Términos y definiciones 60
2. Documentación para nuevos Features 61
3. Git y manejo de versionamiento 63
4. Publicación y procesos automatizados 65
5. Grupos y privilegios 66
6. Documentación de entrega de desarrollos 68
QA & Testing 69
1. Terminología y definiciones 69
2. Ciclo de vida QA 72
2.1. Estudio de requerimientos 73
2.2. Planificación del testeo 74
2.3. Diseño del testeo 76
2.4. Ejecución de las pruebas 77
2.5. Fase de conclusión 78
2.6. Fase de cierre y release 79
MANTENIMIENTO DE SOFTWARE 80
1. Herramientas de monitoreo 80
1.1. Application Insights 80
1.2. Acuetix 81

1.3. Tiempos de mantenimiento 81
GESTION DE INICIDENCIAS 86
1. Roles 86
2. Flujo gestión de incidencias 86
2.1. Recepción de alertas 86
2.2. Clasificación de incidencias 88
2.3. Derivación a Equipo de Seguridad 89
2.4. Reproducción de la incidencia 89
2.5. Desarrollo de la solución 89
2.6. Quality Assurance y testeo de la funcionalidad 90
2.7. Revisión funcional 90
2.8. Notificación a clientes 90
2.9. Monitoreo de la solución 90
3. Procedimientos periódicos 92
3.1. Corrección de vulnerabilidades 93
PLAN DE RECUPERACIÓN DE DESASTRES - DRP 94
1. Terminos y definiciones 94
2. Objetivo 98
3. Supuestos 98
4. Alcance 98
5. Generalidades del plan de recuperación de desastres DRP 99
5.1. Estrategia general de recuperación 100
5.2. Estrategia de acción 100
5.3. Clasificación de los escenarios de desastre 102
5.4. Centro de datos alterno 104
5.5. Canales de comunicaciones 105
5.6. Procedimientos de notificacion, activacion y retorno 106
5.7. Pruebas del plan de recuperación de desastres DRP 121
PLAN DE CONTINUIDAD DEL NEGOCIO - PCN 126
1. Objetivo 126
2. Definiciones 126
3. Desarrollo 127
3.1. Generalidades 127
3.2. Plan de continuidad del negocio 128
3.3. Metodología 130

Figuras

Figura 1 - Organigrama área TI GeoVictoria 7
Figura 2 - Arquitectura interna de la solución 11
Figura 3 - Arquitectura GeoVictoria USB 22
Figura 4 - Diagrama de componentes de código GeoVictoria USB 23
Figura 5 - App con telefono en modo avión 32
Figura 6 - Servicio de sincronización de ítems pendientes 32
Figura 7- Reporte de sincronización con ítems pendientes 33
Figura 8 - Reporte de sincronización sin ítems pendientes 33
Figura 9 – Ejemplo de POST realizado a la API de conexión 34
Figura 10 – POST con credenciales encriptadas 35
Figura 11 – Db browser for Sqlite 35
Figura 12 – Registros de intento de marcaje 36
Figura 13 – Registros de inicio de sesión 36
Figura 14 – Ejemplo de marcación en rango de 39
Figura 15 – Arquitectura base IVR 43
Figura 16 - Detección rápida de errores 48
Figura 17 - Jerarquía de roles 52
Figura 18 - Disponibilidad básica/estándar 54
Figura 19 - Disponibilidad premium/crítica 55
Figura 20 - Replicación de nodos de instancia y datos 56
Figura 21 - Proceso de recuperación rápida de datos 57
Figura 22 - Work ítems en Azure DevOps 62
Figura 23 - Vista de Kanban en Azure DevOps 63
Figura 24 - Diagrama de GitFlow usado por GeoVictoria 64
Figura 25 - Diagrama de Azure PipeLines 66
Figura 26 - Ejemplo de proyecto en DevOps 67
Figura 27 - Ejemplo de Grupos para un proyecto en particular 68
Figura 28 - Ciclo de vida QA 73
Figura 29 - Ejemplo real de un Test plan e información asociada a su estado 74
Figura 30 - Niveles de testeo 75
Figura 31: Resumen de uno de los test rechazados 78
Figura 32 - Ciclo de aprendizaje de errores 84
Figura 33 - Criterio de clasificación. 89
Figura 34 - Flujo de gestión de incidencia para clientes 91
Figura 35 - Flujo de gestión de incidencia para alerta levantada por el equipo de Customer Experience 91
Figura 36 - Ciclo de vida del prgrama PCN 128
Figura 37 - Relación entre planes de continuidad. 129
Figura 38 - Modelo de procesos. 132
Figura 39 - Proceso de evaluación de riesgos. 135
Figura 40 - Equipos del comité de crisis. 140
Figura 41 - Comunicación entre equipos del comité de crisis. 141

Tablas

Tabla 1 - Riesgos 58
Tabla 2 - Actividades segun contingencia 106
Tabla 3 - Medios de Comunicacion 119
Tabla 4 - Estrategias de continuidad 137
Tabla 5 - Alternativas operacionales 138

USUARIOS Y CLAVES DE ACCESO

En ese apartado se presentará el organigrama del área de TI de GeoVictoria, es esta área quien se encarga de establecer la arquitectura completa de la solución, mantener cada uno de los sistemas que moldean el servicio, generar las políticas de seguridad necesarias para asegurar el buen funcionamiento de cada uno de los sistemas, desarrollar cada uno de los nuevos entregables que dan paso a mejoras en el servicio y salvaguardar el correcto funcionamiento del sistema para cada uno de nuestros clientes.

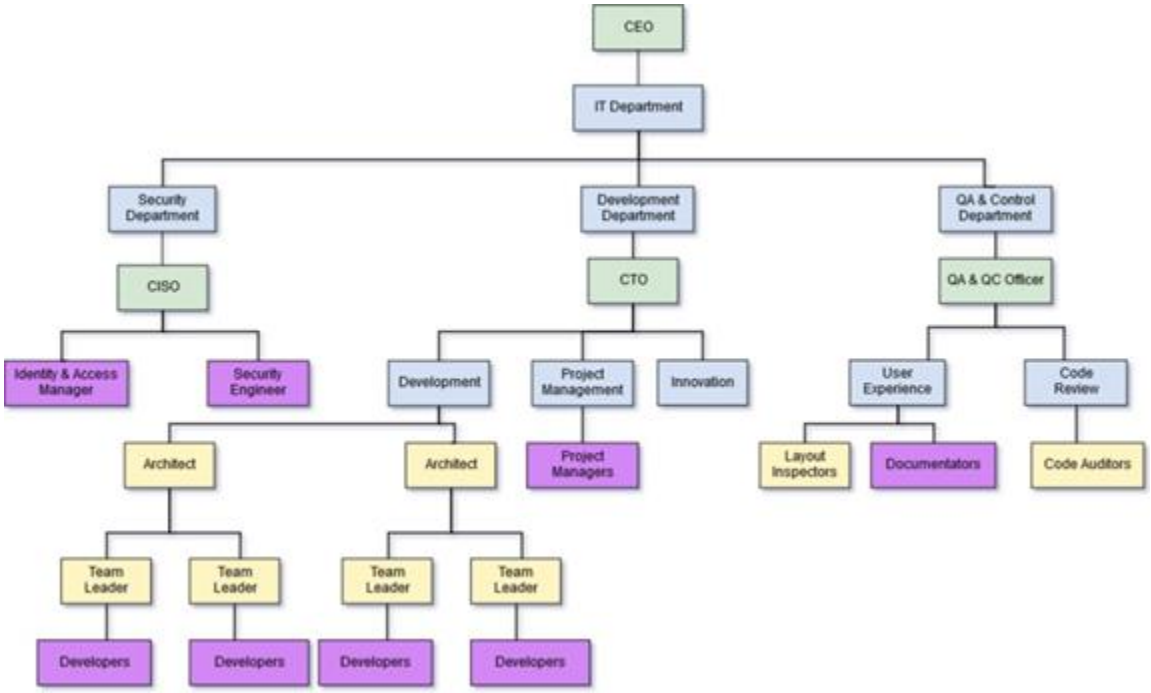


Figura 1 - Organigrama área TI GeoVictoria

Tal como se puede apreciar en el organigrama, existen tres sub-áreas bien definidas las cuales tienen una serie de responsabilidades completamente diferentes entre ellas.

Área de Seguridad: El área de seguridad, se encarga de definir las políticas de seguridad de la organización además de velar por el correcto cumplimiento de dichas políticas, tiene un rol fundamental en el proceso de desarrollo y gestión de incidentes TI

Área de Desarrollo: Es el área encargada de definir la arquitectura de nuestras componentes de software, además de codificar cada uno de los requerimientos que moldean el sistema completo

Área de QA: Es el área encargada de asegurar que cada uno de los entregables producidos por el equipo de desarrollo funcione de la manera correcta, cumpliendo las expectativas de cada uno de los clientes, además de asegurar que se sigan las guidelines de seguridad y arquitectura planteadas por los otros equipos.

1. Herramientas y manejo de usuarios

GeoVictoria es un sistema completamente alojado en la Microsoft Azure, es por esto, que para el desarrollo de las componentes del servicio se utilizan una amplia gama de servicios que, entregados por Microsoft, algunas de las herramientas son:

- Microsoft Azure Portal: utilizada para la administración de los distintos recursos alojados en la nube
- Azure Boards: Administración del proceso de desarrollo
- Azure Repos: Administración de repositorios y versionamiento de código
- Azure Pipelines: Administración de los procesos de publicación e integración continua
- Azure Test Plans: Administración de planes de pruebas y test cases
- Visual Studio: Entorno de desarrollo de software
- Microsoft Teams: Entorno de trabajo colaborativo online

Gran parte de estos servicios componen la suite de herramientas de Azure DevOps, que es uno de los eslabones principales en el proceso de desarrollo de GeoVictoria.

El hecho de utilizar en gran parte herramientas de Microsoft para el uso de cada uno de los recursos del área, nos permite gestionar el manejo de usuarios a través de Azure Active Directory, esto nos permite gestionar cada cuenta de manera centralizada, asignando o removiendo privilegios desde cada uno de los servicios de Microsoft.

Actualmente la organización utiliza autenticación multi factor, para los usuarios administrados a través de Active Directory, utilizando el celular de los usuarios como método secundario de autenticación

2. Acceso a los recursos

Los recursos utilizados por el área de tecnologías de GeoVictoria son entregados exclusivamente a través de privilegios para los usuarios a través de Active Directory, en resumen, tanto los accesos a los componentes de la plataforma, los ecosistemas de bases de datos, el código fuente de cada uno de los servicios de la arquitectura en general, se entrega a través de la asignación de grupos y roles en Azure.

La asignación y administración de estos privilegios es de responsabilidad del área de seguridad informática, la cual entrega los accesos siguiendo siempre la regla del privilegio mínimo, entregando accesos limitados solo a los recursos que la persona en particular necesita.

El área de seguridad informática cada tres meses se encarga de realizar una revisión completa del mapa de privilegios y roles de la compañía, verificando que las asignaciones sean consistentes y que no existan brechas de seguridad sobre los privilegios entregados

3. Llaves de configuración

Cada uno de los subsistemas y servicios en GeoVictoria utilizan una serie de llaves de configuración para acceder a los distintos recursos de cada ambiente de trabajo, estas claves son por defecto secretas y solo los miembros con mayores privilegios de la compañía tienen accesos a dichas claves, dado el nivel de riesgo que estas claves poseen, estas son almacenadas de manera segura utilizando el servicio Key/Vault de Microsoft Azure, el cual además de mantener la información de manera segura permite generar llaves temporales en el caso de que se necesite acceder a dichos recursos sin comprometer la seguridad de las llaves principales

ARQUITECTURA INTERNA DE LA SOLUCIÓN

El presente documento presenta la arquitectura interna de la solución GeoVictoria considerando sus aspectos más relevantes ofreciendo al lector una visión global y comprensible del diseño sobre el cuál se construye y se amplía la solución a través de continuos desarrollos.

El documento pretende entregar información relevante para áreas de TI, Compliance o Security Assesment de las empresas cliente.

1. Alcance

El documento proporciona una visión general de la arquitectura del software GeoVictoria y se detallan algunos aspectos relevantes relacionados con trazabilidad, seguridad, escalabilidad y acuerdos de servicio - SLA.

2. Generalidades

GeoVictoria es una empresa de analítica de fuerza laboral la cual utiliza como entrada para su trabajo el registro y control de asistencia, generando herramientas que permiten mejorar la gestión operativa de sus clientes permitiendo que estos últimos se concentren en el *core* de su negocio, esto prestando un servicio de calidad superior.

Contando con un equipo multidisciplinario de ingeniería, GeoVictoria realiza nuevas implementaciones acorde a las necesidades de sus clientes contando con un equipo de trabajo conformado por Jefes de Proyectos, Ingenieros de Software y Arquitectos de Software, que siguen los lineamientos arquitectónicos plasmados en el presente documento asegurando la fiabilidad del sistema y la información cómo recurso más valioso, de sus clientes.

3. Diagrama General de la Arquitectura de la solución

GeoVictoria está conformado por una serie de servicios alojados en la infraestructura de Microsoft Azure que facilita procesos de actualización de versiones, almacenamiento de información, manejo adecuado de seguridad, facilidad de mantenimiento, escalabilidad, entre otros.
El siguiente diagrama muestra de manera general la arquitectura interna de GeoVictoria y sus principales componentes:

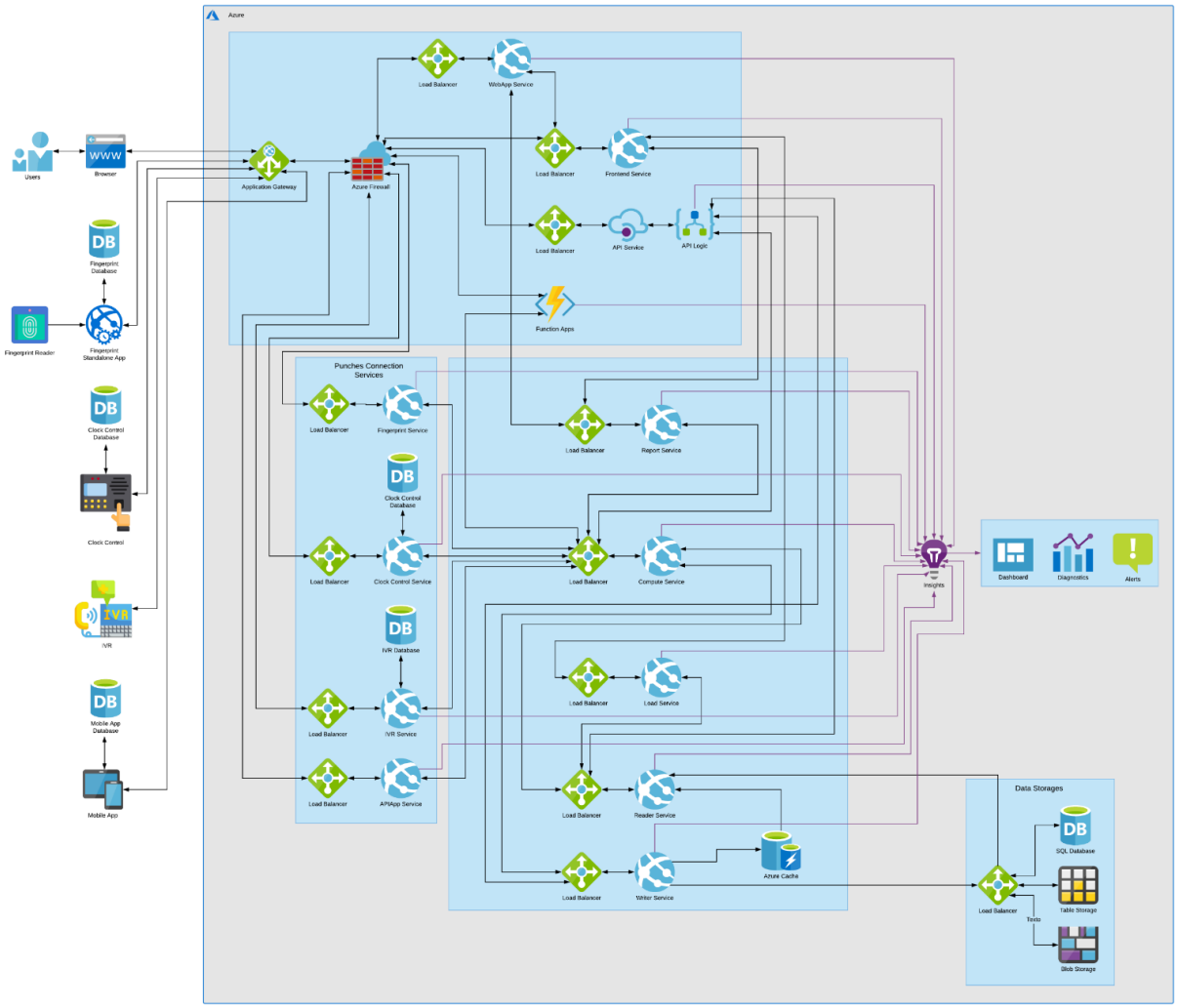


Figura 2 - Arquitectura interna de la solución

Se adjunta versión en PDF del diagrama de arquitectura para una mejor visualización.

Diagrama de arquitectura.pdf

Los principales servicios que conforman la solución GeoVictoria son:

- *WebApp Service*: Ofrece una interface web de usuario para interacción con los usuarios clientes de la solución. La página web ofrecida a través de este servicio cuenta con una serie de reportes de distinta índole, entre los que se pueden mencionar reportes de asistencia, reportes de remuneraciones, reportes legales y de dotación entre otros. Adicionalmente, la página web permite a un administrador generar planificaciones de horario para los usuarios y así dicha información se cruza con las marcas realizadas por los distintos medios para generar un libro de asistencia, el cual indica detalles como retrasos, horas extra, etc. También es posible generar reportes a medida para cada cliente, en los que se acuerda bilateralmente alcances y funcionalidades de estos reportes.
- *Frontend Service*: Ofrece la funcionalidad para generar cada reporte que es solicitado por un usuario a través de la página web de la solución. Se encarga de orquestar los servicios internos de GeoVictoria para acceder a los almacenes de datos y ejecutar la lógica de cálculo de reportes de acuerdo al caso para finalmente tomar el resultado de los cálculos y presentarlos de forma entendible y ordenada al usuario final en una página web, mediante el uso de vistas dinámicas y el uso del lenguaje HTML.
- *API Service*: Servicio enfocado a exponer parte de la funcionalidad ofrecida por GeoVictoria hacía sistemas de los clientes de modo que sea posible integrar los datos obtenidos y procesados por GeoVictoria en una solución propietaria del cliente para manejo de nómina, ERP o lo que el cliente requiera. Este servicio ofrece funcionalidades para la correcta autenticación y autorización de cada cliente para proteger la confidencialidad de sus datos y evitar accesos no autorizados por terceros. El API Service ofrece su funcionalidad a través de la tecnología REST y ofreciendo varios métodos de autenticación cómo clave API (ya en desuso), autenticación basada den token valiéndose de OAUTH 1.0 para ello.
- *Report Service*: Encargado de orquestar la obtención de información, procesamiento de la misma, cálculos y generación de reportes para ser exportados en varios formatos a solicitud del cliente, formatos cómo Microsoft Excel, PDF, XML, CSV, entre otros. El Report Service procesa y genera cada reporte de forma asincrónica evitando así que los servicios solicitantes sean detenidos y sus recursos puedan ser administrados en un ambiente de procesamiento paralelo, para ello ofrece un mecanismo de monitoreo del procesamiento que notifica a los servicios observadores cuando la generación del reporte ha finalizado y ofrece información pertinente para su recuperación del almacén de datos.
- *Compute Service*: Es el servicio de procesamiento de toda la información de GeoVictoria siendo éste el servicio central de GeoVictoria. Este es un servicio que únicamente puede ser accedido por otros servicios de la plataforma y su funcionalidad es ofrecida hacía fuera del entorno de Microsoft Azure únicamente por los servicios WebApp, API y Functions Apps. Dentro de las principales funcionalidades del Compute Service están el cálculo del libro de asistencia para todos los usuarios

de marcaje por todos los medios ofrecidos (Standalone App, Mobile App, IVR y Clock Control), esto teniendo en cuenta las particularidades de cada país y de cada cliente para el cálculo de la información cómo horas extra, recargos nocturnos, entre muchos otros.

- *Functions Apps*: Microsoft Azure ofrece el servicio denominado *Functions Apps* que permite desarrollar con más eficacia aplicaciones sin servidor basadas en eventos que pueden o no ser dirigidos a solucionar problemas de orquestación complejos. En la solución de GeoVictoria la tecnología de *Functions Apps* es empleada para la desactivación automática de usuarios, ya que éste es un proceso de verificación continua del estado de los mismos y sin intervención humana, según la fecha de terminación del contrato, también se emplea para la programación y envío de alertas por correo electrónico, generación de información para plataformas de demostración y *Quality Assurance*, algunas funcionalidades programadas (*sheduled*) para clientes específicos, entre otros usos, facilitando así la automatización de estas tareas de forma eficaz y eficiente y sin la necesidad de realizar desarrollos complejos para lograr estos objetivos debido a que *Functions Apps* ha sido probado y verificado por el equipo de Microsoft y por miles de usuarios alrededor del mundo.
- *Load Service*: Ofrece funcionalidades para cargar alto volumen de datos hacía los almacenes de información de GeoVictoria de forma asincrónica y sin interferir con el correcto funcionamiento del resto de la solución, este servicio es usado únicamente a través del Frontend Service.
- *Reader Service*: Es el único servicio que accede a los almacenes de datos de GeoVictoria y ofrece a los demás servicios la consulta de variados almacenes cómo base de datos SQL Server for Azure, Blob Storage y Table Storage, su funcionalidad para acceso a nuevas fuentes de datos puede ser extendida sin afectar al resto de la solución. La funcionalidad del Reader Service accede a los datos de forma eficaz y eficiente mediante procesos asincrónicos facilitando que los servicios solicitantes puedan ser liberados y aprovechados durante el tiempo que un almacén de datos es accedido, en ningún caso este servicio puede modificar los datos consultados.
- *Writer Service*: Es el servicio complementario al Reader Service ya que este permite la adición, actualización o borrado de la información en los almacenes de datos de GeoVictoria cómo base de datos SQL Server for Azure, Blob Storage y Table Storage. El Writer Service puede ser expandido en su funcionalidad para actualizar nuevas fuentes de datos sin afectar el resto de la solución.

La solución GeoVictoria cuenta adicionalmente con cuatro servicios disponibles para los métodos de marcaje ofrecidos a los clientes, los servicios para este fin son:

- *Fingerprint Service*: Ofrece la comunicación con aplicaciones *standalone* que controlan y toman la información desde un lector de huellas con conexión USB y conectado a un computador. Se encarga de registrar las marcas creadas por los clientes mediante un lector de huellas y cuenta con una base de datos local para almacenar dichas marcas en caso de desconexión, el Fingerprint

Service permite la sincronización entre la información almacenada localmente y los almacenes en Microsoft Azure de la solución de GeoVictoria cuando la conexión se ha reestablecido.

- *Clock Control Service*: Ofrece la comunicación con un reloj de control y mediante él registrar las marcas de los usuarios para ser almacenadas en GeoVictoria y posteriormente ser procesadas para la generación de reportes. Los relojes de control usan una base de datos interna que permite almacenar las marcas cuando la conexión con el servicio no es posible y de este modo cuando se reestablece la comunicación el Clock Control Service se encarga de sincronizar la información almacenada localmente por el reloj de control con los almacenes de datos de GoeVictoria, evitando así la pérdida de información de marcas de los usuarios en casos de eventos de desconexión.
- *IVR Service*: Ofrece la funcionalidad de marcaje a través de una llamada telefónica que reconoce al usuario mediante análisis de voz y registrando la posición geográfica desde la cuál se realiza la llamada (previo registro del teléfono fijo usado o mediante GPS para teléfonos móviles).
- *APIApp Service*: Ofrece la comunicación con la aplicación móvil de GeoVictoria para IOS o Android para registrar marcaciones de los usuarios. Similar a los dos primeros servicios de marcaje este cuenta con una base de datos local para almacenar la información de marcaciones en escenarios desconectados y el APIApp Service ofrece la funcionalidad para sincronizar la información entre la base de datos local de la aplicación móvil con los almacenes de datos de GeoVictoria cuando se recupera la conexión con los servicios de Microsoft Azure.

Todos los servicios ofrecidos por GeoVictoria son multi-instancia de acuerdo a las necesidades del negocio y a la carga generada por los clientes, de modo que cada servicio cuenta con un balanceador de carga configurado para garantizar la disposición 24 horas al día todos los días del año de cada servicio.

Para el almacenamiento de los datos GeoVictoria hace uso de tres servicios de Microsoft Azure que usa de acuerdo a la naturaleza del dato, los almacenes usados son:

- Base de datos SQL Server for Azure: Almacenamiento relacional de la información del negocio y sus clientes.
- Table Storage: Almacenamiento de datos masivos que no requieren de indexación para su uso sino únicamente su particionamiento de acuerdo al uso específico que se le dará y así poderla consultar de forma eficiente y eficaz.
- Blob Storage: Almacenamiento de información sin formato dado pero que tiene alta demanda de espacio para su almacenamiento y facilidad para su posterior ubicación y recuperación.

4. Monitoreo Logs y Alertas

Para el monitoreo de todos los servicios de GeoVictoria se emplea el servicio de Azure llamado Insights que es un servicio orientado a desarrolladores y que les proporciona las herramientas para analizar las aplicaciones, detectar errores en las mismas, problemas de rendimiento e información de uso para análisis de rendimiento. La documentación oficial del servicio Insights puede ser consultada en la página de Microsoft: https://docs.microsoft.com/es-es/azure/application-insights/app-insights-overview. Todos los servicios de GeoVictoria están conectados al servicio Insights registrando allí toda su actividad en forma de logs y registrando información adicional del comportamiento de los mismos cómo registro de diagnóstico, tiempos de respuesta, niveles de éxito, telemetría personalizada de cliente y servidor, segmentación por ubicación del cliente, versión del navegador y otros, y excepciones de servidor y cliente.

El servicio Insights cuenta además con funcionalidad para generar alertas por varios medios al equipo administrador de GeoVictoria cuando ocurren eventos disruptivos o problemas de rendimiento y así, el equipo de Continuidad Operativa puede tomar las acciones correctivas a la brevedad durante las 24 horas del día.

Adicionalmente los servicios de GeoVictoria registran sus propios logs para trazabilidad de las operaciones realizadas y posterior análisis en caso de presentarse fallas o lentitud en el sistema y poder realizar un análisis forense de lo ocurrido. Todos los días el equipo de Continuidad Operativa de GoeVictoria revisa toda la información en Insights y en logs para todos los endpoints, la analiza y en caso de presentarse algún inconveniente dicho equipo genera mantenimientos correctivos priorizándolos de acuerdo a su impacto al negocio. Igualmente, el equipo de Continuidad Operativa analiza el rendimiento general de cada servicio con el fin de generar recomendaciones sobre escalabilidad de los servicios acorde a la demanda presentada o a eventos previamente conocidos que podrían influir en el rendimiento del sistema en un momento dado.

5. Mecanismos de Seguridad

La seguridad es una prioridad en GeoVictoria y esto se ve reflejado en sus desarrollos y en la publicación en producción de sus servicios. Dado que todos los servicios de cara al cliente están alojados en Microsoft Azure se utilizan los mecanismos ofrecidos por esta infraestructura para garantizar al máximo la seguridad de la información y la confidencialidad de los datos.

En el diagrama de arquitectura general de la solución se observa que todo acceso desde el exterior debe llegar primero al Application Gateway de modo que ningún otro componente es expuesto directamente

para evitar intrusiones, adicionalmente luego del Gateway las peticiones pasan a un Azure Firewall configurado acorde a las necesidades de GeoVictoria y en el cuál se habilitó el módulo ofrecido por Microsoft Azure de verificación de vulnerabilidades OWASP, filtrando de éste modo muchos de los posibles ataques de seguridad conocidos.

Aprobada cada petición por el Azure Firewall es redirigida a un balanceador de carga correspondiente al servicio solicitado, son pocos los servicios conectados directamente al Firewall de modo que los servicios críticos del sistema se encuentran en una capa interna que es de acceso restringido y no accesibles desde el Firewall, los servicios más cercanos a este son los destinados a presentación y con poca lógica de negocio.

Para todas las comunicaciones hacía y desde los servicios en Microsoft Azure se realizan a través de HTTPS y toda la información se transmite cifrada desde la fuente (con cifrado TLSv1.2), siendo esta posible fuente un dispositivo de marcaje o una aplicación de GeoVictoria instalada en un equipo móvil o remoto del cliente.

Dado que las vulnerabilidades de seguridad no se presentan únicamente en la infraestructura de la solución también se chequean los nuevos desarrollos realizados por solicitud de los clientes con la herramienta Acuneticx, dicha herramienta verifica todo el código fuente en busca de vulnerabilidades conocidas y almacenadas en librerías públicas de OWASP y en caso de encontrar posibles fallas en el código de seguridad genera las recomendaciones de cada caso para solucionarla, en ese momento el equipo de desarrollo de GeoVictoria analiza los resultados generados por Acuneticx y hace un plan de corrección de fallos.

Las bases de datos cuentan con restricción de acceso, escritura y lectura mediante distintos niveles de autorización, controladas igualmente desde el servicio Azure por estar estas alojadas en la nube. Microsoft incluye tecnologías de seguridad de red y bloqueo de ataques en sus servicios.

6. Escalabilidad

Una de las ventajas de usar la infraestructura de Microsoft Azure es la posibilidad de escalar los servicios de GeoVictoria de forma eficaz y efectiva para afrontar el crecimiento de clientes del negocio y los nuevos requerimientos que exige el mercado. A continuación, se describen las estrategias de escalamiento usadas.

6.1. Automática

La escalabilidad automática se da cuando Microsoft Azure detecta que una o más instancias de un servicio está presentando problemas de rendimiento y se deben tomar acciones para mitigar el impacto al negocio. Los criterios de escalabilidad automática se parametrizaron en Microsoft Azure de acuerdo a los requerimientos del negocio y cómo resultado del análisis de la información de trazabilidad obtenida por los procesos de monitoreo de los servicios. Dentro de los parámetros generales configurados se encuentran los límites de carga de cada servicio que superados obligan a la creación de nuevas instancias del servicio por parte de Microsoft Azure, esto sucede de manera inmediata garantizando la alta disponibilidad del servicio y los SLA con los clientes.

Para GeoVictoria la escalabilidad automática es aplicada únicamente cómo escalabilidad horizontal y ésta se presenta cuando el monitoreo continuo indica que hay congestión inusual de un servicio y supera los límites pre-establecidos, razón por la cual automáticamente Microsoft Azure decide automáticamente crear nuevas instancias del servicio hasta que se pueda atender toda la demanda, siempre asignando la misma cantidad de recursos a cada nueva instancia creada. De igual forma la escalabilidad horizontal puede dar de baja algunas instancias de un servicio cuando el mismo tiene poca demanda y se están desperdiciando recursos innecesariamente.

La parametrización pre-establecida para el escalamiento horizontal es actualizada con base a los análisis de los datos recolectados en *Applications Insights* y en los *logs* del sistema de modo que continuamente se puedan ajustar las instancias en *release* de los servicios y contar así con alta disponibilidad de todo el sistema.

6.2. Manual

En algunas ocasiones particulares se puede pronosticar un eventual aumento en la demanda de servicios por parte de los clientes, puede ser por temas de carácter social (días festivos, fiestas nacionales, cambios presentados en la sociedad por pandemias, entre otros), por temas propios del negocio cómo eventos especiales de algunos clientes que generarán una alta demanda del servicio en unas fechas determinadas o también por crecimiento continuo de la base de usuarios clientes del sistema.

Estos eventos de rara ocurrencia deben ser analizados por el equipo de GeoVictoria para medir el impacto al negocio y genera un plan de acción para ajustar las instancias de los servicios temporalmente y de forma manual para afrontar cada evento, estos ajustes pueden implicar la escalabilidad manual horizontal o vertical de los servicios o inclusive una estrategia combinada de los dos tipos.

Igualmente, tras superarse el evento de rara ocurrencia se debe manualmente restaurar la configuración habitual para reléase de los servicios y llevar todo el sistema a su comportamiento habitual y adecuado para siempre prestar un servicio de alta disponibilidad.

7. Acuerdos de servicio - SLA

El acuerdo de nivel de servicio con los clientes o SLA es un contrato que describe el nivel de servicio que un cliente espera de su proveedor, en este caso de GeoVictoria.

Según el *Information Technology Infrastructure Library* (ITIL) se definen tres tipos de SLA:

- SLA de servicio: Es un SLA aplicable a todos los clientes que contraten los mismos servicios, es llamado generalmente SLA Estándar. Cuando la empresa ofrece diferentes tiempos de resolución y respuesta ante eventos disruptivos es necesario entonces crean un SLA individual por cada servicio ofrecido a sus clientes.
- SLA basado en el cliente: Es un SLA aplicable a todos los servicios contratados por un mismo cliente o por un grupo de clientes o una misma área de negocio. En éste tipo de SLA se definen tiempos de resolución y respuesta propios para cada cliente de acuerdo a las negociaciones especiales que le apliquen.
- SLA multinivel: Es un SLA que combina los dos primeros tipos y evitan conflictos entre SLA previamente existentes al generar un único SLA que cubra tanto a los servicios contratados cómo a las necesidades particulares de cada cliente.

GeoVictoria establece SLA de servicio para todos sus clientes ya que a todos se les ofrece una alta disponibilidad del servicio por igual apoyado en los múltiples mecanismos de redundancia de servicios mediante la escalabilidad ofrecida por Microsoft Azure e independizando la operación del negocio de las instalaciones físicas donde se desempeña el personal de GeoVictoria, en el peor de los casos de eventos disruptivos el servicio seguirá disponible y los dispositivos de marcaje continuarán almacenando localmente la información de los usuarios en caso de desconexiones temporales cómo se describió anteriormente en el presente documento.

Los SLA basados en el cliente y los SLA multinivel no son aplicados en GeoVictoria dado que todos los clientes son una prioridad para la empresa y todos merecen por igual un servicio de calidad y alta disponibilidad independiente de la cantidad de empleados que tenga el cliente, de su país o de sus condiciones individuales.

7.1. Monitoreo de los acuerdos de servicio - SLA

El *Service Level Management* es el proceso de gestión de los SLA y se encarga de definir, documentar, acordar, monitorear, medir, reportar y revisar el nivel de cada servicio ofrecido ofreciendo ventajas competitivas para la empresa.

La buena aplicación del *Service Level Management* permite a GeoVictoria:

- Acordar condiciones realistas que la empresa pueda soportar.
- Conocer las expectativas de los clientes.
- Establecer parámetros concretos para medir el estado de los servicios.
- Cumplir con los plazos y condiciones acordadas con los clientes.
- Evitar conflictos futuros dado que el SLA permite la comunicación preventiva con el cliente y genera confianza en el mismo.

Para la generación de SLA viables en GeoVictoria se analizan los servicios prestados cómo la estructura interna de la organización para poder cumplirlos. Con el fin de analizar los servicios se generó un catálogo de servicios para entender la relación de cada uno de ellos con la organización y sus equipos de trabajo y además los procesos que se llevan a cabo para ofrecer el servicio, el catálogo es ofrecido en la sección “Diagrama general de la arquitectura de la solución” del presente capítulo.

Facilitando las tareas de cumplimiento de los SLA se automatizan y se actualizan continuamente los parámetros que garantizan la estabilidad y rendimiento de los servicios, esto apoyado en *Insights*, *logs* generados y en el equipo de Continuidad Operacional de GeoVictoria que se encarga de la coordinación interna que cumpla con los tiempos de respuesta y resoluciones en coordinación con el equipo de manejo de incidentes descrito en el plan de continuidad del negocio.

Adicionalmente a las herramientas automáticas de medición y a los análisis realizados de la información recolectada se realizan encuesta a los clientes que tienen la última palabra en cuanto a la prestación de los servicios de GeoVictoria, las encuestas pretenden medir el nivel de satisfacción y se realizan mediante encuestas mensuales que se realizan a todos los clientes cuando ingresan por primera vez en el mes a la plataforma web de GeoVictoria, todos los resultados obtenidos son almacenados en Microsoft Azure y posteriormente se genera un informe consolidado y dirigido al equipo directivo de la empresa para ser analizado y para la toma de decisiones.

Cómo mecanismo alternativo para la realización de encuestas los Jefes de Proyecto periódicamente realizan encuestas más enfocadas a cada cliente apoyados en el conocimiento del cliente y de sus

necesidades, luego consolidan la información recolectada y presentan un informe que muestre el nivel de satisfacción del cliente, resultados complementarios a los obtenidos con las encuestas automáticas aplicadas mensualmente.

8. Alta disponibilidad y hot swap

Para garantizar la alta disponibilidad del servicio todos los servicios de GeoVictoria se encuentran publicados en la infraestructura de Microsoft Azure generando un primer nivel de alta disponibilidad garantizada por Microsoft contando con múltiples centros de datos alrededor del mundo y alta replicación de servicios y datos a través de ellos, considerando así posibles pérdidas por desastres naturales, ataques vandálicos, daños a sus equipos entre muchos otros eventos disruptivos.
Aprovechando la infraestructura de Azure la solución de GeoVictoria cuenta con mínimo una instancia principal de cada uno de sus servicios y una instancia réplica en un centro de datos alterno, en caso de falla del primero el segundo entra a operar de forma inmediata sin interrupción del servicio y sin pérdida de datos dado que Azure garantiza la replicación de los almacenes de datos entre centros de datos. Cómo un nivel adicional de aseguramiento de la información el equipo de GeoVictoria realiza respaldos periódicos de todos los almacenes de datos en caso de ser necesaria una restauración manual de los servicios, esto cubierto dentro del plan de recuperación de desastres descrito en capítulos posteriores.

Cuando se publica un nuevo cambio hacía producción se aprovechan los mecanismos de entorno diferenciales de Microsoft Azure para publicar por cada uno de los servicios una nueva instancia incluyendo los nuevos cambios hacía el ambiente de *staging*, allí se realizan las pruebas finales de funcionamiento e integración y en caso de ser superadas se procede mediante herramientas de Azure a reemplazar las instancias corriendo en ambiente productivo *release* por las nuevas instancias aprobadas en ambiente *staging* mediante un *hot swap*, de éste modo en ningún momento se deja de prestar el servicio dado que cada instante habrá una o más instancias del servicio corriendo y atendiendo las peticiones de los clientes.

Al finalizar el proceso todas las instancias del servicio en ambiente *release* serán reemplazadas y el cambio no es observable por los clientes ni afectado su rendimiento.

ARQUITECTURA DE LOS METODOS DE MARCAJE

La siguiente sección presenta en detalle la arquitectura de cada método de marcaje, con sus propias cualidades específicas de manera de que se pueda entender a cabalidad el funcionamiento de cada uno de ellos.

1. GeoVictoria USB

GeoVictoria USB es una solución para el registro de asistencia mediante huella digital, el cual sólo necesita un lector de huellas y un computador Windows con conexión a internet. La misma engloba el proceso de marcación que consiste en la lectura de la huella dactilar del usuario en uno de los dispositivos equipados con esta capacidad y la comprobación de que la misma esté registrada en el sistema, para luego guardar en base de datos la marca que se está realizando.

Para ello existe un aplicativo cliente que se instala en un computador del usuario final, al cual se le conecta el dispositivo USB capaz de leer huellas dactilares y este conjunto terminal con conexión a internet es capaz de conectarse con los servidores de GeoVictoria para el intercambio de información. Esta arquitectura será descrita de forma ampliada posteriormente.

El proceso de marcación por esta vía necesita de varios requisitos, entre ellos se encuentran los requisitos de hardware constituidos por el artefacto lector de huellas, el computador y la conexión a internet, mencionados anteriormente, además de los requisitos funcionales. Estos constituyen varios pasos que se chequean antes de realizar la operación de marcaje. El primero es la comprobación de que el identificador del huellero se encuentre registrado en el sistema. Este identificador es una cadena alfanumérica de 9 caracteres separadas por guiones cada 3 posiciones, y es vital para el buen funcionamiento de la marcación que esté asignado al grupo de marcaje al cual pertenece el usuario.

El segundo paso es el chequeo de la huella dactilar leída. Esta debe encontrarse registrada en el sistema, si no lo está el usuario debe pasar por un proceso de enrolamiento para hacer este registro efectivo, este proceso de enrolamiento puede realizarse directamente del conjunto formado por el huellero USB y el computador donde el software se encuentra instalado. Cumpliendo estos dos requisitos funcionales es posible realizar marcaciones a través de GeoVictoria USB.

La utilización de este método de marcación es más común en locales donde el proceso de entrada y salida ocurre en un solo lugar, y que el mismo esté dotado técnicamente, entiéndase un computador, para la implantación de esta tecnología. Por ejemplo, un escritorio de conserjería, un mostrador, un puesto de mando, un puesto de control de acceso, etc.

1.1. Arquitectura

Como ya se ha mencionado, a grandes rasgos esta solución está formada por un dispositivo USB lector de huellas dactilares y un computador con conexión a internet. Para establecer visualmente una disposición de los principales componentes que intervienen en todos los procesos de GeoVictoria USB se muestra la siguiente imagen:

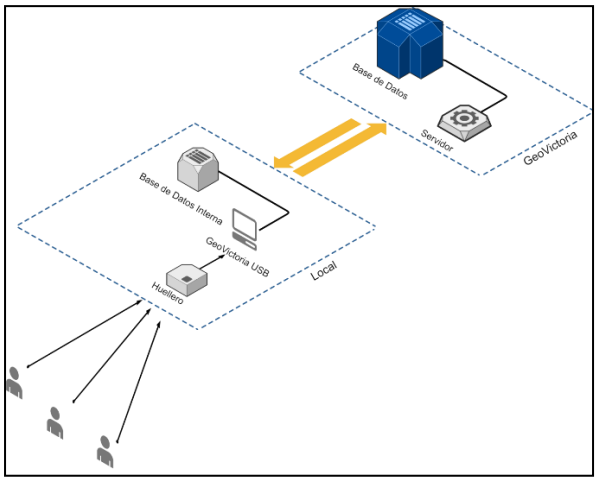


Figura 3 - Arquitectura GeoVictoria USB

Como se puede observar cada uno de los huelleros que se encuentran conectados a GeoVictoria USB poseen una conexión directa a los servidores de GeoVictoria a través de este software. Además, cada una de estas estaciones de trabajo cuenta con una Base de Datos local, la cual cumple un papel fundamental con los problemas de sincronización que puedan ocurrir y a la hora de cualquier fiscalización de datos que se necesite. Esta arquitectura entrega en particular sistema eficaz de tolerancia a errores, los cuales pueden estar dados fundamentalmente por desconexiones, intentos de marcas fallidos o incluso ambas , esto ya que, si existiera algún inconveniente que impidiera la conexión directa del GeoVictoria USB con los servidores centralizados, el sistema sigue registrando las marcaciones localmente y luego que se restablezca la conexión con los servidores sincronizará enviando todas las marcas que se encuentren pendientes de envío.

Una vez generadas las marcas, estás son enviadas a GeoVictoria a través del AppService "*FingerPrint Service*" que se encarga de generar la comunicación entre la infraestructura del cliente con el servidor, además se encarga de realizar los procesos necesarios para la correcta contabilización de la marca en las bases de datos y por ende en las distintas secciones de la plataforma web.

1.2. Escalabilidad

La arquitectura de GeoVictoria USB está pensada para ser ampliamente modificable y tan a la medida como cada cliente necesite. Pues está basada en MVC(Modelo-Vista-Contralor) y con la implementación de los patrones de diseño Factory, Facade y Encapsulamiento montados sobre

Windows Forms, hacen que el núcleo principal de la solución pueda permanecer inalterable, al tiempo que se pueden agregar módulos que atiendan a las necesidades más específicas de cada cliente.
En el siguiente diagrama de paquetes se puede observar la relación entre los distintos módulos:

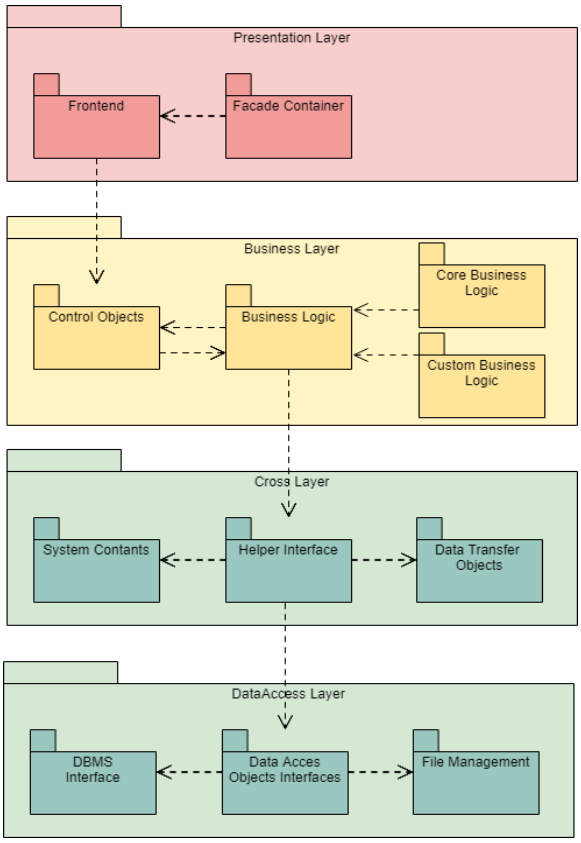


Figura 4 - Diagrama de componentes de código GeoVictoria USB

Como se puede observar en el diagrama anterior en la capa de negocio hay una diferenciación entre toda la lógica que responde a necesidades específicas de nuestros clientes y la lógica principal de la solución. Así se logra mantener esta última inalterable a cualquier posible cambio de escalabilidad y al mismo tiempo proveyendo la facilidad de crecer en el volumen de funcionalidades a la medida.

Adicionalmente en la capa de acceso a datos, la interfaz DataBase Management System (DBMS Interface) permite la diversidad de conexiones con gestores de base de datos y por consiguiente realización de operaciones con ellos. Si bien GeoVictoria USB utiliza principalmente SQLite para la gestión de su base de datos interna y sus procesos, esta interfaz está abierta a la posibilidad de escalar la solución y adecuarla a integraciones con otros sistemas gestores de base de datos que puedan existir en el terminal de los clientes. De esta forma si la solución necesita integrarse con algún otro aplicativo con el que tenga que coexistir lo puede hacer a través de base de datos, pudiendo leer directamente de cualquier otro DBMS ajeno, siempre que se creen las funcionalidades necesarias para ello en esta

interfaz. Por ejemplo, tenemos algunos casos de éxito en integraciones de este tipo que varían desde SQL Server hasta Visual Fox Pro.

1.3. Lenguajes y entornos

La aplicación cliente de GeoVictoria USB está desarrollada fundamentalmente utilizando el lenguaje de programación C#. Pues al estar creada la solución sobre el framework .NET, se vale de sus librerías tanto para la capa de presentación como para la capa de acceso a datos.

El Front End en la capa de presentación utiliza las librerías gráficas Windows Forms de .NET para crear todas las vistas con las que interactúa el usuario final. Por su parte en el acceso a datos se utilizan librerías acordes a este proceso para SQLite, así como el modelo LINQ para poder hacer consultas sobre los datos ya extraídos de los distintos espacios de almacenamiento.

Mientras que, del lado del servidor, el servicio de conexión se encuentra desarrollado en C# con .Net Core y montado en Azure App Services.

1.4. Seguridad

La seguridad de GeoVictoria USB se puede evidenciar en varios aspectos de la solución. Por ejemplo, en la autenticación de usuarios que realiza el terminal en el cliente para poder dar como válido un proceso de marcaje. Este proceso, como ya se explicó, consta de varios requisitos para que se pueda realizar. Los cuales son: la comprobación de que el identificador del huellero se encuentre registrado en el sistema y que la huella dactilar leída se encuentre registrada en el sistema.

La conexión en el sistema de marcación instalado en las dependencias del cliente y los servidores en la nube de GeoVictoria se realiza de manera cifrada utilizando protocolo HTTPS mediante certificados SSL, además como medida adicional de seguridad solo es necesario que el firewall de las redes clientes soporte la conexión con una única url, la cual es utilizada para realizar la completa sincronización del dispositivo, esto ayuda a que no exista la posibilidad de que atacantes externos intercepten la comunicación entre el dispositivo y los servidores

Todos los datos sensibles se encuentran cifrados en reposo, de manera de poder acceder desde las dependencias del cliente a los datos identificables de cada trabajador, además es importante señalar que el sistema en ningún momento guarda alguna imagen biométrica de la huella dactilar de los usuarios al realizar su marcación, sino que solo almacena un Hash encriptado con algoritmos de propiedad de los proveedores de hardware por lo cual ni siquiera el personal de GeoVictoria tiene la capacidad de reconstruir una imagen de la huella.

2. GeoVictoria BOX

GeoVictoria Box corresponde a un sistema de marcaje realizado a través de dispositivos biométricos instalados directamente en las dependencias del cliente, estos dispositivos, solo requieren de una fuente eléctrica y una conexión a internet para poder funcionar.

Los dispositivos de marcajes utilizados por GeoVictoria pueden poseer diferentes tipos de validación, siendo la marcación a través de huella dactilar la más comúnmente utilizado, sin embargo, dentro de los métodos de validación a elegir se encuentran:

- Validación de Huella Dactilar
- Validación Facial
- Validación de Palma
- Tarjetas de Proximidad
- Marcación según identificador

GeoVictoria no se encarga de fabricar los dispositivos utilizados, sino que, utiliza como proveedor a ZKTeko es esa empresa la que se encarga de realizar los desarrollos que deban estar dentro de los dispositivos mismos, estos se encargan de agregar nuevas funcionalidades, modificaciones en el firmware, etc. GeoVictoria mantiene una estrecha relación comercial con este proveedor, y los desarrollos de nuevas funcionalidades se realizan a través de un proceso de solicitud formal siguiendo protocolos impuestos por ellos.

La empresa ZKTeko es la encargada de realizar las pruebas de sus dispositivos, para así asegurar la calidad de cada uno de estos, una vez llegado a GeoVictoria este se revisa y testea para ver si cumple con lo solicitado al proveedor, en caso de no ser así se devuelve explicando cada uno de los problemas encontrados en el proceso de aseguramiento de calidad del dispositivo. Todo esto es parte del protocolo que provee ZKTeko para sus desarrollos.

2.1. Arquitectura

El sistema se compone de distintos elementos, tanto físicos como lógicos, estos son Reloj Control, Reloj Control Server y GeoVictoria, los cuales serán descritos a continuación:

- **Reloj Control:** Corresponde al dispositivo de control de asistencia. El dispositivo se conecta vía HTTPS a Reloj Control Server. Existen dos tipos de tecnología para la conectividad de los Relojes: GPRS/3G y LAN.
- **Reloj Control Server:** Servidor que recibe y procesa los datos hacia y desde los relojes control, cumpliendo el rol de interfaz centralizada para toda la operación.
- **WebApp:** Plataforma interna que procesa la información de las marcas recibidas desde todas las plataformas de marca de GeoVictoria. Esta información se inserta directo en la base de datos SQL Server alojada en Azure a la que tiene acceso este servicio Cloud. Este servicio tiene toda la información del sistema, su administración, generación de reportes, entre otros.

El servidor de Reloj Control está desarrollado sobre una WebApi (C# .NET) montada en un App Service en Azure. Esta tiene la capacidad de escalarse de manera horizontal ya que cuenta con un balanceador de carga que distribuye los Requests entre todas las instancias activas. Dado esto, se tiene la capacidad de recibir conexiones de una cantidad muy grande de relojes de manera simultánea, con la posibilidad de crecer de manera eficaz, segura y sin impacto en la calidad de servicio.

2.2. Disponibilidad del Servicio

La disponibilidad del servicio, el balanceo de carga y redundancia están asegurados, debido a que el servicio es proporcionado por Azure. El servidor de Reloj Control es ServerLess (desde el punto de

físico) existe una probabilidad mínima de que el servidor de marcas se descomponga ya que todo nuestro sistema está en la nube(montado en tecnologías ServerLess), en caso de que esto suceda nuestra recuperación no afectara en gran medida a nuestra continuidad de servicio ya que bastara con republicar el proyecto para volver a tener en línea el servidor, en el intertanto los relojes seguirán almacenando las marcas y estas serán sincronizadas en el momento en el que el servidor vuelva a estar disponible.

En caso de que el reloj control se queme la probabilidad de perder marcas es el mínimo ya que este envía las marcas constantemente, así mismo estas se procesas con una cola y se suben inmediatamente ya que todo nuestro sistema está constantemente en línea, de todas maneras, el cliente puede comprar relojes para utilizarlos en caso de emergencia, y tenerlos como reemplazo físico cuando corresponda.

El SLA de GeoVictoria asegura una uptime de los servicios un 99.9% del tiempo. Para la plataforma Box, independiente de la conectividad a internet, el sistema permite la marcación y sincronización posterior de los datos.

GeoVictoria Box posee una serie de procesos de monitoreo en el caso de que pase alguna de las condiciones anteriormente mencionadas, de entro de estos podemos definir procesos de monitoreo automáticos, los cuales permiten a nuestro equipo tener registro del estado actual de los dispositivos y de las situaciones que acontecen en el día a día en los mismos. Estos son:

- **Alerta dispositivo con memoria llena:** Esta alerta se envía cuando los dispositivos se encuentran con su capacidad de memoria por sobre del 90%.
- **Alerta de desconexión:** Esta alerta se envía cuando nuestro sistema percibe que un reloj se desconecta (independiente de qué tipo de desconexión sea).
- **Comprobación de marcas:** Este se realiza para comprobar que todas las marcas realizadas en un reloj se subieron correctamente a nuestro sistema.

Además de los procesos automáticos, GeoVictoria Box cuenta con los siguientes procesos manuales los cuales consisten en las acciones que se toman cuando hay que realizar trabajos en terreno, dentro de estos se encuentran:

- **Recuperar Marcas vía USB:** este proceso requiere de un técnico o usuario con conocimiento sobre este proceso. Este ingresa un dispositivo USB (pendrive) e inicia un proceso en el cual se guardan las marcas seleccionadas por la persona (por lo general dentro de un rango de fechas o todas las marcas del reloj). Posteriormente en caso de una falla de internet con el reloj estas se pueden subir masivamente por medio de nuestra página web en el módulo respectivo. En caso de ser de una alerta de reloj por memoria llena estas se guardan para tener un respaldo de dichas marcas.

- **Reinicio manual del reloj:** en caso de algún fallo del reloj, este se puede reiniciar de forma remota, en caso de que este reinicio no se pueda dar o no pueda arreglar, un técnico irá a terreno a revisar el reloj.

2.3. Seguridad

Al igual que en GeoVictoria USB, toda la información sensible en reposo se encuentra cifrada en las bases de datos internas de cada dispositivo, con la salvedad adicional que GeoVictoria no es capaz de acceder a los dispositivos con privilegios superiores por lo cual no es posible para rescatar información directamente desde el dispositivo sin utilizar alguna de las interfaces entregadas por ZKTeko.

La conexión entre el dispositivo de marcaje se realiza de manera cifrada utilizando protocolo HTTPS mediante certificados SSL y al igual que en GeoVictoria USB solo es necesario dejar el libre paso en el Firewall del cliente a una url de GeoVictoria, en esta url se encuentra el servidor de conexión de los relojes control y se encarga de la sincronización completa de las operaciones con el dispositivo.

Por último, sea cual sea el tipo de verificación que este utilizando el dispositivo en particular (huella, rostro, palma, etc) GeoVictoria solo maneja minucias de las características biométricas, lo que implica que en ningún caso es posible para la organización tener imágenes o datos de las características biométricas completas de cada uno de los usuarios que realizan su marcaje a través de los dispositivos.

3. GeoVictoria APP

GeoVictoria cuenta con una aplicación móvil disponible tanto para Android como para iOS, en las tiendas Play Store y App Store respectivamente, que permite al usuario, entre otras cosas, realizar su marcación de asistencia diario con geolocalización, marcación de actividades, revisar el historial de marcas realizadas, así como también revisar los turnos planificados para el usuario durante la semana y más.

GeoVictoria siempre se encuentra innovando e implementando nuevas funcionalidades en la aplicación móvil. La inclusión de estas funcionalidades está sujeta a la política de desarrollos de GeoVictoria que incluye una etapa para discutir y levantar el requerimiento, la etapa de diseño, la etapa de implementación y un riguroso proceso de QA que garantiza que la liberación de la aplicación a la fase beta contenga el menor número de bugs. GeoVictoria se reserva el tiempo en el que la aplicación liberada estará en fase beta dependiendo entre otras cosas de la complejidad del desarrollo y la retroalimentación recibida por los testers internos y externos.

Aparte de la liberación de nuevas funcionalidades, es posible que sea necesaria la liberación inmediata de correcciones de bugs que sean reportados por nuestros usuarios. En este escenario la política es, recibir la notificación de posible bug, analizarlo, reproducirlo, desarrollar una solución, probarla debidamente y enviarla al proceso de QA de HotFixes, para posteriormente liberarla en la tienda de aplicaciones respectiva.

Los requisitos mínimos de uso de la aplicación según sistema operativo son los siguientes:

Android:

- Android 4.1 o superior.
- Procesador de 500MHz o superior.
- 750Mb de RAM o superior.
- GPS y cámara de selfie (de usar validación por selfie).
- Conexión a internet.
- Cámara de selfie de 1 Mp o más (en caso de utilizar reconocimiento facial)

IOS:

- IOS 9 o superior
- IPhone 4S o superior

3.1. Arquitectura

Tal como los demás métodos de marcación GeoVictoria APP se compone de una interfaz de trabajo con el usuario, en este caso una aplicación móvil, una API que realiza la comunicación y sincronización de la información y el mismo sistema de almacenamiento central en la nube.

La aplicación es la que permite al usuario realizar su marcaje. A su vez consta de las interfaces necesarias para permitirle a los usuarios utilizar cada una de las características que la aplicación provee, una base de datos interna para almacenar localmente todos los datos que maneja la aplicación incluyendo las marcas y un set amplio de servicios de sincronización de datos para subir marcas, ubicaciones e informes hacia GeoVictoria y descargar información de usuarios y planificaciones hacia la aplicación.

La interfaz de programación de aplicaciones (API), que consta de una serie de servicios que permiten la comunicación entre la aplicación y GeoVictoria. Estos servicios se encuentran ejecutándose en Azure en una infraestructura de alta disponibilidad. Entre los servicios más importantes se encuentran el de inicio de sesión que permite al usuario autenticarse, el procesamiento de marcas que recibe las marcas desde la app y gestiona su almacenamiento en la base de datos de GeoVictoria, el procesamiento de informes y el de ubicaciones que recibe desde la app informes en base a fotografías tomadas por el

usuario y las ubicaciones capturadas por el GPS del dispositivo respectivamente para almacenarlas en la base de datos de GeoVictoria y el de data check al que cada cierto tiempo la aplicación se conecta para preguntar si existen o no cambios en los datos del usuario y sus planificaciones para descargarse los últimos cambios de ser necesario.

3.2. Lenguaje y entornos

La aplicación de marcación de GeoVictoria está desarrollada en lenguaje nativo. En el caso de Android se usa Kotlin en más del 90% del código, que es un lenguaje moderno, fuertemente tipado y 100% compatible con java; y que es de propiedad de Google. Para su desarrollo utilizamos Android Studio como entorno de programación.

La aplicación de iOS está desarrollada 100% en Swift utilizando como entorno de desarrollo Xcode.

3.3. Comunicación

La comunicación entre cada uno de los actores que forman parte de la solución de GeoVictoria App se encuentra cifrada con SSL (ver sección de inicio de sesión).

Además, todos los accesos a los servicios de la API por medio de la aplicación se encuentran debidamente autenticados y autorizados, de tal manera que si, por ejemplo, un usuario que ha iniciado sesión correctamente pierde la autorización al uso de la aplicación, a pesar de tener la aplicación ejecutándose, la API denegará cualquier comunicación entrante desde esta sesión mientras que la aplicación mostrará en pantalla al usuario un mensaje de error de autenticación/autorización.

Como ejemplo importante de la conexión entre el dispositivo móvil y los servidores de GeoVictoria se presenta a continuación el flujo de inicio de sesión.

3.3.1. Flujo de inicio de sesión

Para hacer uso de la aplicación móvil el usuario debe iniciar sesión adecuadamente. El proceso de inicio de sesión consta de dos fases: autenticación y autorización.

En la fase de autenticación, el usuario debe ingresar sus credenciales, esto es, el nombre de usuario y la contraseña asignadas por el administrador. Inmediatamente después de presionar sobre el botón de iniciar sesión la contraseña ingresada es encriptada haciendo uso del algoritmo criptográfico AES-256

y una solicitud es generada hacia el servicio de inicio de sesión de la API de la aplicación utilizando el protocolo HTTPS para la comunicación.

El servidor se encargará de revisar estas credenciales para comprobar si pertenecen a un usuario activo. Para esto se cuenta con una base de datos que contiene la información de los usuarios de GeoVictoria. Si es así, el proceso de inicio de sesión pasará a la siguiente fase, de lo contrario la autenticación falla y se denegará el acceso.

La siguiente fase es la de autorización, para esto, el servidor determinará si el usuario al que le pertenecen las credenciales validadas en la fase anterior está autorizado para utilizar la aplicación como método de marcaje. Un usuario está autorizado si es que la empresa tiene contratado el servicio de GeoVictoria App y además el administrador permitió el uso de la aplicación para este usuario. Esta validación es determinante para permitir o no el acceso en conjunto con la autenticación.

En la autorización también se determinará a qué características tendrá acceso el usuario, por ejemplo, si la validación en el marcaje se hará por reconocimiento de rostros, si tiene acceso a realizar marcación en cuadrilla, etc. Esta verificación se realiza consultando a la base de datos de Servicios Contratados.

Si el proceso de autenticación y autorización se completa correctamente, tanto el nombre de usuario como la contraseña encriptada son almacenadas en la base de datos local de la aplicación para su posterior acceso, y la aplicación procederá a mostrar la interfaz inicial designada para la marcación, de lo contrario, las credenciales son descartadas y la aplicación mostrará un mensaje de error en la interfaz de inicio de sesión.

Una vez que la aplicación se encuentra con una sesión iniciada, levantará un servicio que se encargará de verificar cada cierto tiempo si existen cambios en los datos del usuario o de sus planificaciones de turno.

Esta verificación se realiza a través de la API generando un código hash de los datos que se encuentran almacenados en la base de datos de la aplicación y comparándolos con el código hash generado por la API y calculado en base a los datos del mismo usuario almacenados en la base de datos de GeoVictoria.

Si ambos hashes son diferentes, entonces la aplicación generará una solicitud a la API pidiendo por datos actualizados de usuario o de planificaciones de turno según sea el caso. La API a su vez pedirá esta información a la base de datos de usuarios y planificaciones respectivamente.

Estas solicitudes son debidamente autenticadas con las mismas credenciales que se almacenaron en la base de datos de la aplicación durante el proceso de inicio de sesión.

3.4. Disponibilidad del servicio

Al igual que el resto de los servicios de GeoVictoria en la nube, la API para aplicaciones se encuentra en una arquitectura de clústeres que garantiza una alta disponibilidad, tal que, si una de las instancias falla, se levante automáticamente en unos pocos segundos la instancia del cloud service que se encontraba en estado pasivo.

Adicional a esto, la API se encuentra funcionando en los servidores de Azure que garantizan un uptime del 99.97%.
Aún en el posible evento de que la API no responda por un tiempo determinado, las marcas realizadas en ese lapso y que no pudieron subir inmediatamente a GeoVictoria quedarán almacenadas en la base de datos de la aplicación y se levantará un servicio que intentará sincronizar estas marcas cada 15 minutos de manera automática. De esta forma se garantiza que no exista pérdida de datos.
En la siguiente imagen se muestra la aplicación funcionando en modo avión.



Figura 5 - App con telefono en modo avión

La imagen a continuación muestra el servicio de sincronización de ítems pendientes ejecutándose.

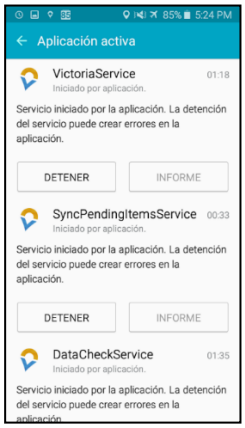


Figura 6 - Servicio de sincronización de ítems pendientes

En la siguiente imagen se puede visualizar el reporte de sincronización de la aplicación en un teléfono celular que se encuentra en modo avión, se ha generado un informe y una marca que no han sido sincronizadas y al intentar sincronizar la aplicación arroja error de red.

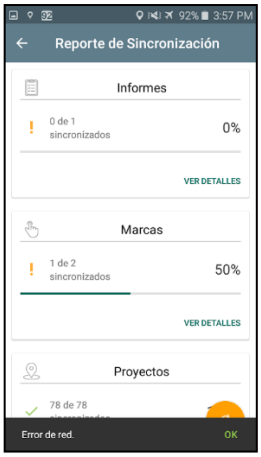


Figura 7- Reporte de sincronización con ítems pendientes

En la siguiente imagen, luego de recuperar la conexión a internet y esperar alrededor de 15 minutos, y volviendo a ingresar al reporte de sincronización, se puede visualizar que los ítems pendientes se han sincronizado correctamente.

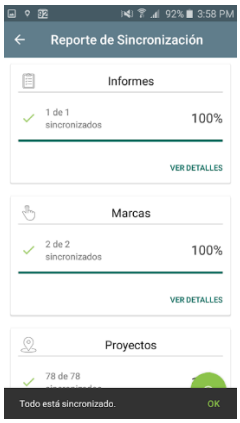


Figura 8 - Reporte de sincronización sin ítems pendientes

3.5. Seguridad

El acceso a la información a través de la aplicación está debidamente autenticado y autorizado, siendo el enfoque de la aplicación es el registro de asistencia por lo que tanto si un administrador como un usuario normal inician sesión sólo podrán ver su propia información y siempre que tengan activado ambos la opción de “permite uso de la aplicación” en la página web.

La aplicación de GeoVictoria tanto para descargar como para enviar datos se comunica con los servicios de GeoVictoria a través de una interfaz de programación de aplicaciones (API), esta comunicación se encuentra cifrada utilizando el protocolo https para impedir que estos datos puedan ser interceptados e intervenidos.

La siguiente imagen muestra un request típico hecho desde la aplicación a la API de GeoVictoria para consultar información, donde se puede visualizar que la conexión es hecha a través del puerto 443, es decir https.

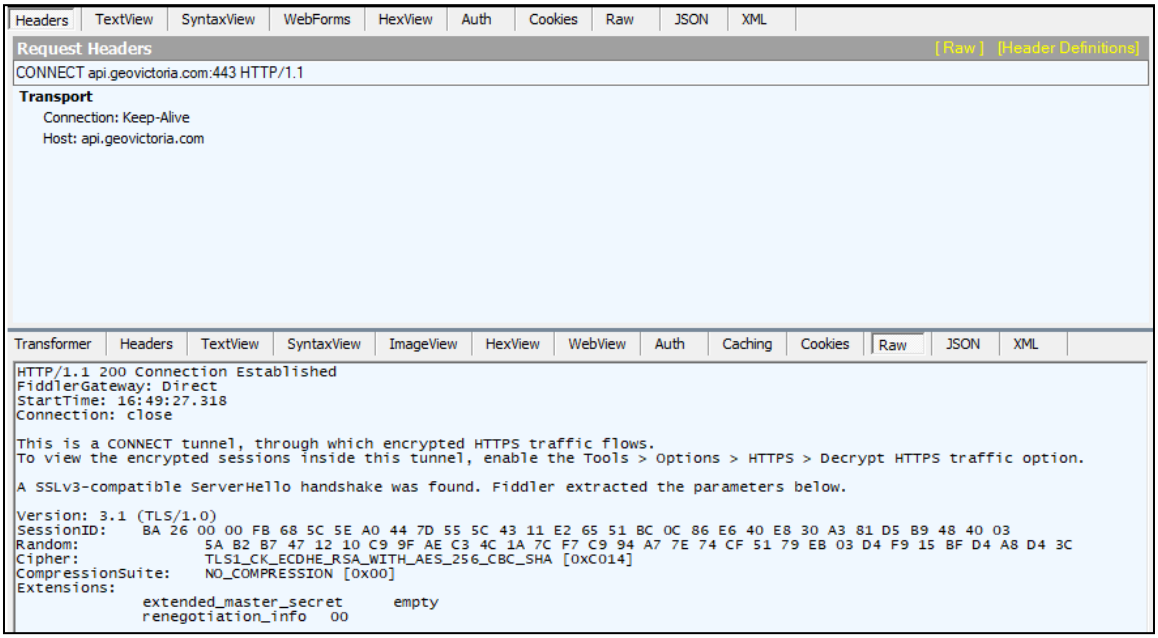


Figura 9 – Ejemplo de POST realizado a la API de conexión

Además, cada solicitud hecha por la aplicación a la API lleva las credenciales cifradas con AES, de tal forma que se autentique cada solicitud para poder procesarla.

La siguiente imagen muestra un request hecho desde la App, donde se puede visualizar las credenciales del usuario cifradas con AES 256. Este request fue capturado en un ambiente controlado donde a propósito se desactivó https para poder visualizar los datos enviados.

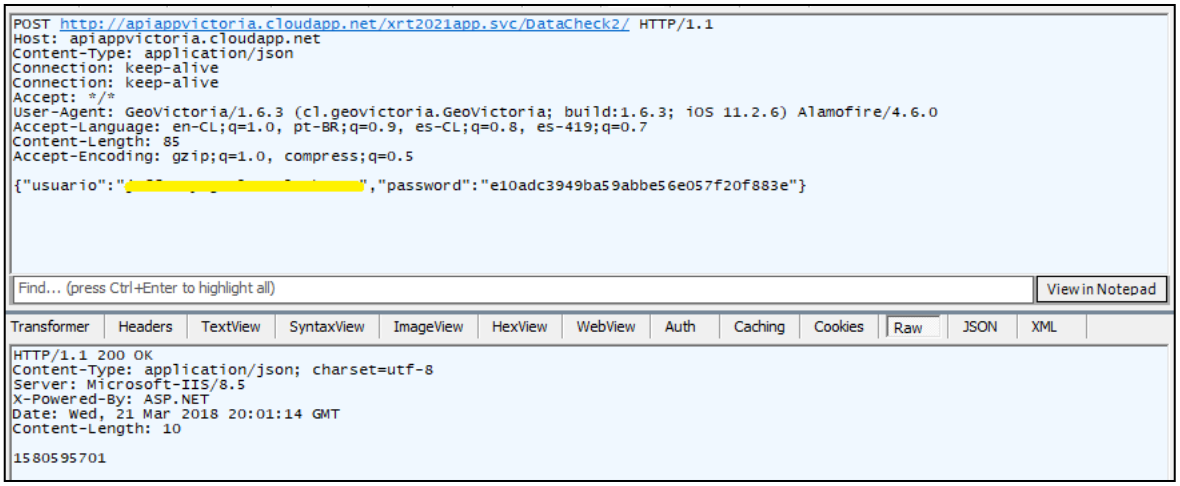


Figura 10 – POST con credenciales encriptadas

Los datos almacenados en la aplicación son inaccesibles por terceros debido a la propia seguridad incluida en los sistemas operativos iOS y Android. Sin embargo, existe un proceso que permite enviar estos datos a un almacenamiento en línea de GeoVictoria, estos datos son solo accedidos por personal autorizado de GeoVictoria y además se encuentran cifrados.

La siguiente imagen muestra el programa Db Browser for SQLite utilizado para visualizar la información de los datos de la aplicación solicitando la Key para desencriptar estos datos y poder visualizarlos.

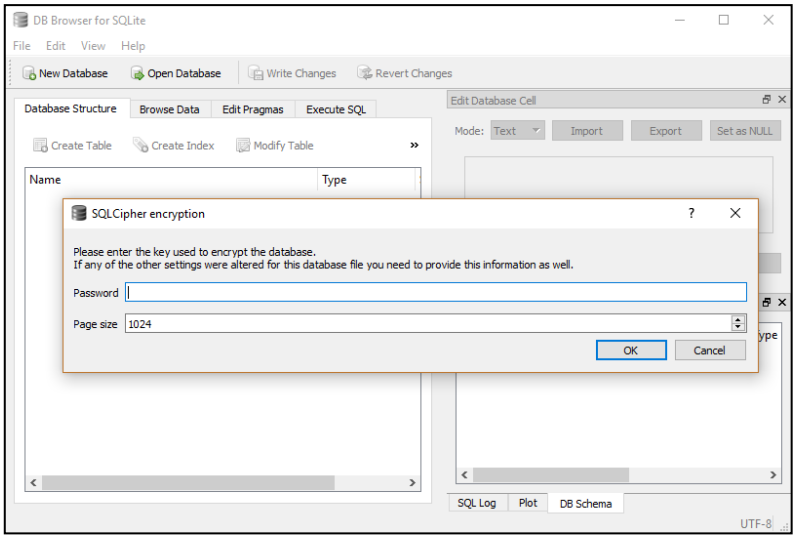


Figura 11 – Db browser for Sqlite

También, como medida de seguridad, se registran las actividades realizadas en la aplicación como marcaciones, intentos de marcación, informes, turnos, entre otros.

Por ejemplo, en la siguiente imagen se puede visualizar registros de intentos de marcaje hechos desde la aplicación.

Prueba Usuario (77.777.777-6)

Fecha	Tipo de Intento	Razón de la Falla
21-03-2018 10:24:54	Fallido	Patrón erróneo
21-03-2018 10:24:55	Fallido	Patrón erróneo
21-03-2018 10:24:58	Fallido	Patrón erróneo
21-03-2018 10:25:00	Fallido	Patrón erróneo
21-03-2018 10:25:04	Fallido	Patrón erróneo
21-03-2018 16:27:40	Fallido	Patrón erróneo
21-03-2018 16:27:44	Fallido	Patrón erróneo
21-03-2018 16:27:46	Fallido	Patrón erróneo
21-03-2018 16:27:48	Fallido	Patrón erróneo
21-03-2018 16:27:53	Fallido	Patrón erróneo
21-03-2018 16:27:54	Fallido	Patrón erróneo

Figura 12 – Registros de intento de marcaje

Cada usuario que inicia sesión en la aplicación posee un perfil en GeoVictoria que define a qué funcionalidades tendrá acceso, por ejemplo si es un supervisor de un grupo que está activado para cuadrillas, la aplicación descargará los datos de los usuarios a los cuales tiene bajo su cargo; o si el grupo tiene configurado el seguimiento por GPS, la aplicación activará el servicio de seguimiento para enviar coordenadas GPS del usuario a GeoVictoria y poder visualizar su desplazamiento en un mapa.

Además, el evento de inicio de sesión de un usuario en la aplicación queda registrado en las bases de datos de GeoVictoria, guardando el identificador interno del usuario, la versión de Android y modelo de teléfono desde donde inició sesión, última fecha de inicio de sesión y la última fecha de cierre de sesión de modo que se pueda validar desde qué equipo el usuario se encuentra marcando.

Id_Usuario	Android_Version	Device_Model	Login_Date	Logout_Date
317847	24	HUAWEI MHA-L09	Sat Feb 10 10:15:32 GMT-03:00 2018	Sat Feb 10 10:15:10 GMT-03:00 2018

Figura 13 – Registros de inicio de sesión

3.5.1. Validación de Identidad

Para que la marcación se lleve a cabo el administrador podría habilitar la característica de validación de marcaje que le permitiría verificar si la marca fue realizada por la persona que dice haberla hecho.

La verificación puede realizarse de manera activa o pasiva, Dentro de los métodos de validación pasiva se encuentran:

- Validación por firma: la validación por firma permite al usuario registrar su firma al momento de marcar, la misma que podrá ser revisada posteriormente por el administrador desde el detalle de marca en el portal web.
- Validación por selfie: la validación por selfie permite al usuario registrar su selfie al momento de marcar, esta foto podrá ser revisada por el administrador desde el detalle de marca en el portal web.

Por otro lado, los métodos de validación activos son los siguientes:

- Validación por patrón: la validación por patrón consiste en enrolar un patrón de puntos similar al patrón de bloqueo en Android que se usará posteriormente para validarse al marcar. Internamente, el patrón de puntos se almacena encriptado con el algoritmo AES-256 en la base de datos local de la aplicación y se sube a GeoVictoria de la misma manera.

- Validación por reconocimiento de rostros: La biometría de rostros consiste en enrolar un rostro utilizando el servicio de reconocimiento de rostros de Microsoft Face API que se utilizará posteriormente para validarse contra las selfies tomadas al momento de marcar. La Face API permite detectar una o varias caras humanas en una imagen y obtener rectángulos faciales donde se encuentran las caras en la imagen, junto con atributos faciales que contienen predicciones de características faciales basadas en aprendizaje automático. Las características de atributos faciales disponibles son: edad, emoción, sexo, postura, sonrisa y vello facial, junto con 27 puntos de referencia para cada cara de la imagen.

3.5.2. Utilización del GPS

Es requisito para las marcaciones realizadas a través de la aplicación de GeoVictoria contar con las coordenadas GPS que indiquen dónde fueron efectuadas. De aquí que los equipos móviles, para poder utilizar la aplicación, deben contar con GPS funcionando.

Además, para mejorar la precisión de la ubicación obtenida, la aplicación de GeoVictoria se valdrá de las siguientes fuentes:

- GPS
- Datos móviles
- Wi-Fi

Esto es muy útil para marcaciones realizadas en lugares cerrados donde el GPS podría no tener cobertura.

De aquí que, para poder marcar, es necesario que el usuario tenga al menos activados en su equipo cualquiera de las siguientes opciones:

- Tener GPS y datos móviles activados
- Tener GPS y Wi-Fi activados

En otras palabras, si el usuario desactiva el GPS durante el proceso de marcación la aplicación no le permitirá marcar y le pedirá que active el GPS en el dispositivo. O también si el usuario tiene activado el GPS, pero tiene tanto datos móviles como Wi-Fi desactivados o en modo avión tampoco se le permitirá marcar.

GeoVictoria además provee el servicio de seguimiento (tracking) que permite al administrador conocer en todo momento, durante la jornada laboral de los usuarios, conocer su posicionamiento

Tomando en cuenta que la obtención de la ubicación podría ser un proceso lento, la aplicación de GeoVictoria levanta un servicio en segundo plano para tal efecto desde el momento en el que el usuario presiona el botón de marcar entrada o salida. Es decir, mientras el usuario se encuentra realizando el proceso de validación, la aplicación está usando todas las fuentes disponibles, sea GPS, datos móviles o Wi-Fi para obtener la ubicación más precisa y en el menor tiempo posible.

Si después de la validación, aún no ha sido posible encontrar la ubicación, la aplicación asignará 6 segundos adicionales al proceso de obtención de ubicación, mostrando en pantalla un mensaje al usuario indicando que está en proceso de obtener una ubicación para la marca.

Si luego de estos 6 segundos no se ha podido obtener una ubicación, entonces la aplicación permitirá al usuario elegir si desea reintentar con 6 segundos adicionales o marcar sin asociar una ubicación.

Además, es importante indicar que, para mayor precisión y control de errores, el tiempo de vida de una ubicación obtenida por el GPS y guardada en memoria por la aplicación es de 15 segundos, por lo que, cumplido este tiempo, si la aplicación necesita leer la ubicación desde la memoria del dispositivo, la invalidará y procederá a obtener una actualizada.

Para entender un poco más lo indicado en el último párrafo consideremos el siguiente ejemplo: supongamos que, durante el proceso de marcación, la aplicación obtuvo la ubicación inmediatamente después de presionar sobre el botón entrada o salida, el usuario se tomará un tiempo para lograr validarse, el cual podría superar los 15 segundos indicados. Suponer además que el usuario se encuentra en movimiento, por lo que después de los 15 segundos la ubicación obtenida podría no ser tan precisa. Es por este motivo que la ubicación obtenida es invalidada y la aplicación necesitará obtener una actualizada.

3.5.2.1. Bloqueo por ubicación

Esta característica permitirá a un administrador restringir el marcaje a los usuarios en un radio geográfico para un día dado; valiéndose de las planificaciones, los grupos y el GPS del dispositivo móvil.

GeoVictoria cuenta con una funcionalidad llamada: planificación por grupos. Esta funcionalidad permite al administrador, además de agregar un turno a una planificación en un día dado, adicionarle también un grupo, lo que se traduciría a: un usuario para un día dado tiene asignado un turno dado y debe realizar su marcaje en el grupo asignado.

A esto le agregamos que, un grupo puede tener asignada una ubicación y una tolerancia de ubicación del grupo, que se traduce a un radio de acción.

Si juntamos ambas cosas podemos restringir el marcaje a los usuarios en un radio geográfico dado. Esta restricción puede variar día tras día de acuerdo con la planificación asignada.

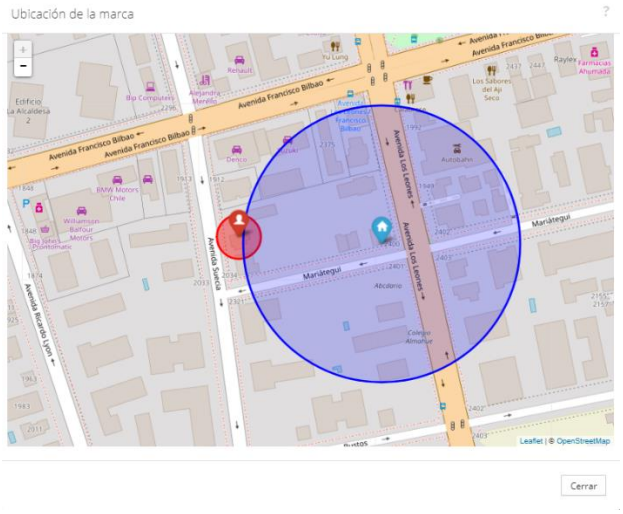


Figura 14 – Ejemplo de marcación en rango de

3.5.2.2. Alteración del GPS

Las marcas del registro de control de asistencia realizadas a través de la aplicación móvil tienen asociada una ubicación: en coordenadas latitud y longitud, obtenidas a través del módulo GPS de los teléfonos celulares.

Esta ubicación podría verse comprometida si los usuarios instalaran y utilizaran aplicaciones de terceros que interceptan y modifican estas coordenadas a fin de simular que el usuario se encuentra en otra ubicación, llamemos a estas aplicaciones fake gps.

Con el auge de aplicaciones como Pokémon Go, que utilizan la ubicación de un usuario en un momento determinado para generar la estrategia del juego, se popularizó este tipo de aplicaciones que falsean coordenadas GPS a fin de dar al usuario cierta ventaja sobre el juego.

GeoVictoria también podría verse afectada por este tipo de aplicaciones por lo que cuenta con esta característica de bloqueo que detecta si la ubicación asociada a una marca de asistencia es de procedencia real (del GPS del dispositivo) o simulada por una aplicación de terceros, a fin de bloquear el marcaje para este último.

Podemos dividir la amplia gama de celulares con sistema operativo Android en dos tipos: los rooteados y los no rooteados. Se dice que un celular es rooteado cuando ha sido intervenido por un usuario a fin de tener acceso a configuraciones avanzadas del sistema operativo. Un usuario con estos accesos y los conocimientos necesarios puede realizar una amplia gama de tareas administrativas en su teléfono celular, incluyendo la posibilidad de simular ubicaciones y enmascararlas como reales (como si fuesen obtenidas del GPS) sin que haya forma de detectarlo, sin embargo, rootear un dispositivo puede ser causa para la pérdida de la garantía de este por lo que es una opción poco usada por los usuarios.

No podemos dar una solución para este tipo de dispositivos por lo que, de aquí en adelante, nos centraremos en los dispositivos no rooteados que son mayoría.

Para que una aplicación fake gps pueda falsear una ubicación, necesita que el sistema operativo Android le conceda el permiso de ubicaciones simuladas, el cual es activado por el usuario a través del modo desarrollador del dispositivo.

Android permite saber si el permiso de ubicaciones simuladas está activado, si el equipo tiene instalada alguna aplicación que haya requerido el permiso y le da la posibilidad al fabricante de habilitar una configuración, para saber si una ubicación es generada por el GPS o si es simulada.

Sin embargo, no todos los fabricantes habilitan la configuración indicada y, aun así, aquellos que la habilitan generan falsos positivos. En las pruebas realizadas con equipos

Samsung, 2 de cada 10 ubicaciones simuladas generadas fueron etiquetadas como “reales” (del GPS).

GeoVictoria implementa como solución bloquear la realización de las marcaciones si existe en el teléfono alguna aplicación que esté utilizando el permiso de ubicaciones simuladas, mostrando en pantalla al usuario qué aplicaciones instaladas le impiden continuar con el proceso de marcaje y generando una alerta de marca fallida al correo electrónico del usuario, cuya razón además puede ser visualizada desde el portal web.

Además, cabe indicar que, existen aplicaciones incluyendo aplicaciones de los fabricantes, que utilizan el permiso de ubicaciones simuladas para otros fines.

Para sobrellevar el caso de las aplicaciones de los fabricantes, GeoVictoria agrega a la solución la posibilidad de mantener una lista blanca de apps que requieren permisos de aplicaciones simuladas, tal que, si un usuario tiene instalada una de estas aplicaciones, no sea tomada en cuenta como fake gps.

La lista blanca puede aplicarse a nivel global (todas las empresas), a nivel de empresa o a nivel de usuario.

3.6. Monitoreo y Alertas

La aplicación está diseñada para soportar marcación fuera de línea. Cuando un usuario marca sin internet la sincronización fallará y los datos de marca permanecerán seguros en la aplicación siempre y cuando ésta no sea eliminada, desinstalada o el usuario cierre sesión de manera forzada. Esto es muy útil en ambientes de escasa o nula cobertura de datos donde es imprescindible proveer al usuario de funcionalidades críticas como lo es el marcaje de asistencia aun cuando las condiciones no son las ideales.

Si la sincronización falla, la aplicación levantará el servicio de sincronización de ítems pendientes que se encargará de intentar sincronizar todo aquello que no haya sido sincronizado aún cada 15 minutos y se detendrá sí y solo si detecta que ya ha sincronizado todo. Este servicio se ejecutará aun si el usuario cierra la aplicación.

Si el servicio de sincronización falla al sincronizar por tres ocasiones seguidas, entonces intentará también enviar la base de datos de la aplicación para salvaguardar las marcas por si el error va más allá de un tema de conexión a internet.

GeoVictoria cuenta con un repositorio general y de acceso únicamente a personal autorizado donde se almacenarán estas bases de datos muy útiles en resolución de errores y en recuperación de información.

Además, la aplicación implementa el servicio de Crashlytics de Fabric que es una solución de reportería de errores que nos informa de fallos en la aplicación. Nos proporciona un detalle de los errores que ocurrieron en la aplicación, definiendo la clase, la cantidad de incidencias e incluso la descripción del error. Toda esta información puede ser filtrada por versión, sistema operativo, incidencias, usuarios afectados, etc. También, permite analizar en tiempo real información de uso de la aplicación, crecimiento, retención y compromiso.

Por el lado de la API de la aplicación, el acceso a cada uno de los servicios está debidamente registrado pudiendo verificar en todo momento los ítems recibidos desde la aplicación, sean marcas, informes, ubicaciones, etc.; así también como sobre cargas del servicio, escalado automático y posibles errores o fallas que puedan ocurrir.

4. GeoVictoria Call

El servicio GeoVictoria Call consiste en un sistema telefónico que es capaz de recibir una llamada e interactuar con un humano mediante grabaciones de voz, de esta forma se puede marcar asistencia sin tener que incurrir en gastos adicionales correspondientes a dispositivos de marcación, sino que, a través de cualquier línea telefónica disponible. El sistema además permite seleccionar desde que numeración de teléfono puede marcar cada usuario de manera de estar seguros de que la marcación se realiza desde el puesto de trabajo del trabajador o donde este puesto el equipo telefónico desde el cual se le permitió marcar.

Las marcas realizadas a través del sistema GeoVictoria Call son almacenadas en la misma base de datos centralizada de marca cumpliendo con las mismas medidas señaladas en los otros métodos de marcación.

4.1. Arquitectura

La aplicación se compone de un servidor cliente (IVR Client) que procesa los datos de voz enviados por la red telefónica, un servidor Asterisk que proporciona las funcionalidades de una PBX (central telefónica), y de la interconexión con la red telefónica conectada al PSTN mediante FXS.

Todos los procesos realizados por el sistema de IVR son automatizados, por lo que no existen procesos manuales en su ejecución. Todos los componentes nombrados anteriormente corresponden a nuestra arquitectura de red y la interconexión con los sistemas de telefonía local.

A continuación, presentamos un diagrama general de la arquitectura del servicio GeoVictoria Call:

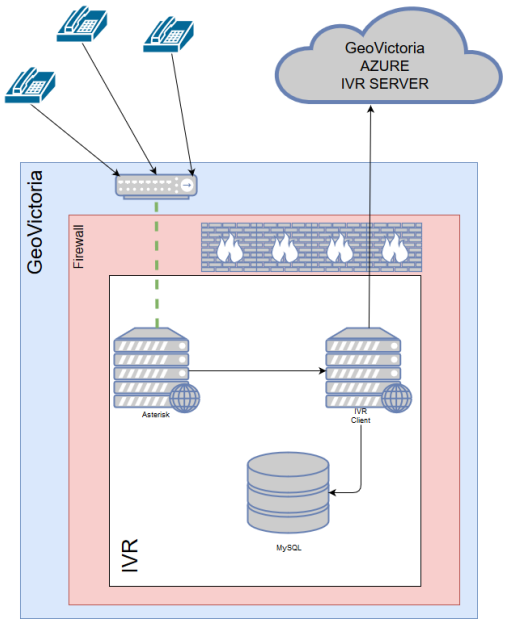


Figura 15 – Arquitectura base IVR

La información de nuestros servidores está protegida por un firewall, que impide el ingreso de cualquier dato que no corresponda a una llamada telefónica voip.

Los componentes principales del sistema son:

- Pstn: central telefónica, se conecta al servidor asterisk, y permite la entrada de llamadas mediante la comunicación en tramas e1 del servicio telefónico.
- Asterisk: pbx utilizada para recibir las llamadas telefónicas mediante protocolo fxs, de telefonía (tramas e1). Ejecuta las aplicaciones de ivr e ivr client, para controlar los flujos de funcionamiento del ivr.
- Ivr client: aplicación que recibe los datos del servidor asterisk. Se integra directamente a través de un script en php que intercambia información con el servidor local.
- Ivr server: este servidor se encuentra alojado en azure y se encarga de procesar la información biométrica y las lógicas de funcionamiento de la aplicación. Se comunica con el ivr client a través de un webservice, protocolo SOAP, con encriptación SSL (https). Este servicio guarda la información en una base datos sql server de la plataforma en azure de geovictoria.
- Geovictoria: plataforma interna que procesa la información de las marcas recibidas desde todas las plataformas de marca de geovictoria. Esta información se inserta en la base de datos sql server alojada en azure, a la que tiene acceso este servicio cloud. Este servicio tiene toda la información del sistema, su administración, generación de reportes, entre otros.

4.2. Disponibilidad del Servicio

El SLA de GeoVictoria asegura una uptime de los servicios un 99.9% del tiempo durante el año. Este uptime es respecto a la posibilidad de marcaje, que se encuentra sujeto a las condiciones mínimas de funcionamiento de la plataforma. En el caso de la plataforma IVR, se debe tener en consideración una posible degradación del servicio debido a la pérdida de calidad de servicio en las líneas telefónicas, congestión, entre otros factores externos al procesamiento biométrico de los audios recibidos en los servidores.

Existen distintos scripts para la restauración del sistema (en PERL) y para la ejecución de rutinas desde los servidores de Asterisk. Los archivos de configuración se generan con el script de restauración del sistema operativo.

En IVR existe una aplicación para seguir la traza de los registros de auditoria. En este se muestra la información de la respuesta entregada por cada etapa de la transacción de marcaje. Esta aplicación es utilizada por el equipo de soporte, con un login asociado para asegurar la protección de los datos.

Los registros de auditoria se guardan tanto localmente en los servidores Linux, como en la nube al consultar las lógicas de negocio. No existen respaldos locales ya que la misma información está disponible en los de la nube.

4.3. Seguridad

Respecto del servicio, la autenticación de dispositivos se realiza mediante el ISDN que viene en la trama de comunicación E1 que viene desde la central telefónica. Esto es el número de teléfono asociado a cada teléfono que llama, que es identificado en el Asterisk.

GeoVictoria permite bloqueo de marcaje si el ISDN no corresponde al valor configurado dentro de la plataforma web, para asegurar que la marca se realice en el lugar físico designado.

Desde el punto de vista de la seguridad de los servidores, todas las comunicaciones internas de la aplicación IVR, que tiene datos sensibles como el Rut de los trabajadores o la grabación de las voces, no puede ser accedido desde afuera de la red. El Firewall protege el sistema de amenazas, y todas las comunicaciones entre aplicaciones se realiza mediante inserción en bases de datos protegidas, o bien WebService encriptados y encapsulados en HTTP vía SSL.

El área de soporte tiene acceso a la plataforma web de GeoVictoria, con perfil de administrador multiempresa. Pueden acceder a la misma información que los clientes dentro de la plataforma, para poder brindar un servicio de calidad, en particular para IVR pueden ver los reportes gestados en la plataforma. escuchar las grabaciones de los usuarios que marcaron en la empresa y administrar las configuraciones del sistema.

Las comunicaciones entre los distintos módulos que componen la solución GeoVictoria Call se encuentran cifradas, además, cada una de las bases de datos tiene las claves y datos importantes cifradas en reposo utilizando AES 256.

La API de interconexión funciona con OAUTH 2, sin token de expiración. Con autorización y autenticación vía credenciales.

ECOSISTEMA DE BASE DE DATOS

Hoy en día, la información es uno de los activos más valioso de las empresas y GeoVictoria es consciente de ello, por este motivo y para satisfacer las necesidades de sus clientes dispone de un equipo de profesionales para la administración y gestión de las diferentes y modernas tecnologías que hay en el mercado.

GeoVictoria, como Partner Gold de Microsoft desde el 2019 (https://partner.microsoft.com/en-us/inspire/awards), aprovecha las ventajas de su plataforma Azure para almacenar los datos de forma que estos estén disponibles en cualquier lugar del mundo a cualquier hora y con el respaldo de la tolerancia a fallos (desastres naturales, falla de hardware, actualización de equipos, etc.). GeoVictoria trabaja para hacer de los datos de sus clientes en información e información en conocimiento.

Una serie de normas y estándares rigen el funcionamiento del ecosistema de base de datos de GeoVictoria.

1. Ambiente

En el desarrollo de aplicaciones y prueba se generan gran cantidad de datos que menguan la capacidad de almacenamiento y velocidad de procesamiento de la base de datos. Es correcto disponer de diferentes ambientes de trabajo a nivel de base de datos para destinar la mejor cobertura a los clientes y evitar una posible manipulación de los datos productivos por error. GeoVictoria establece cuatro ambientes de trabajo, con sus respectivas bases de datos. Los modelos relacionales entre los distintos ambientes van siendo actualizados a medida que se cumplen los requisitos en cada una de las etapas del desarrollo de software y cumplan los rigurosos estándares de calidad de que GeoVictoria solicita en sus aplicaciones.

- **Desarrollo:** Ambiente de trabajo enfocado para las tareas de desarrollo de software o sistemas de información. Los datos que albergan las bases de datos, de este ambiente, son totalmente ficticios. Las bases de datos se encuentran en instancias diferentes de los de producción y pruebas.

- **QA:** Ambiente de trabajo en el que se realizan las pruebas de calidad del software. Ubicado en diferente instancia de desarrollo, concreta sus labores en bases de datos separadas al área de desarrollo, utilizadas únicamente por los profesionales de aseguramiento de calidad. Los datos que albergan estas bases de datos son totalmente ficticios.

- **Sandbox:** Destinado para realizar demostraciones/pilotos con los clientes Sandbox actualiza sus bases de datos cada 3 meses con las de producción. Dicho ambiente no modifica dato alguno de los utilizados ya que están en instancias y servidores diferentes. Además, cuenta con los mismos

desarrollos que alberga el servidor de producción para que sea una copia fiel de lo que el cliente dispondrá al momento de unirse a GeoVictoria.

- **Producción:** La información contenida en las bases de datos de este ambiente corresponden a los generados en los clientes a través de las aplicaciones de GeoVictoria. Dichos datos se ubican en instancias separadas de todos los demás ambientes que existen para no afectar el rendimiento de lectura y escritura. El acceso a los datos es únicamente a través de la plataforma y sigue una rigurosa norma de seguridad de roles de acceso, cifrado de datos transparente y Always Encrypted. Este es el único ambiente en el que se realiza una copia de seguridad de los datos. Cada 15 minutos, de forma incremental, se almacenan éstas en regiones diferentes cumpliendo con los mismos cifrados.

Se debe considerar que los ambientes son actualizados a medida que se superan las pruebas de calidad de GeoVictoria sobre sus aplicaciones. Esto puede conllevar la modificación de tablas, índices, relaciones, etc. en base de datos. Una vez que recibe la aprobación por las áreas correspondientes, se ejecutan los procesos de actualización por instancia, una a la vez, las conexiones entrantes se redirigen a las bases de datos actualizadas hasta que todas cuenten con la modificación correspondiente sin detener el flujo de trabajo.

2. Tipos de base de datos y usos

Cada dato es diferente, unos sirven para diferenciar una entidad, otros con motivos de costos, otros como los datos históricos, etc. Cada dato es analizado y derivado a su lugar de almacenamiento para que no afecte a la velocidad y rendimiento del sistema.

2.1. Bases de datos relacionales

Una pieza clave para el cliente es disponer de sus datos en todo momento. Por este motivo GeoVictoria confía en la tecnología que Azure SQL Database para sus modelos relacionales. La información es almacenada en tablas, las que alimentan el servicio de Intelligent Insights. Azure SQL Database consta de una memoria caché que almacena la información en base a los reportes entregados por Insights. Otra de las ventajas del uso de Azure SQL Database es la temprana detección de errores o potenciales errores en tablas, columnas y/o celdas de la base de datos. El servicio de Insights notifica e intenta reparar el posible bloqueo. Por motivos de consistencia las consultas y/o escrituras a estos datos son denegadas mientras la corrección es realizada.

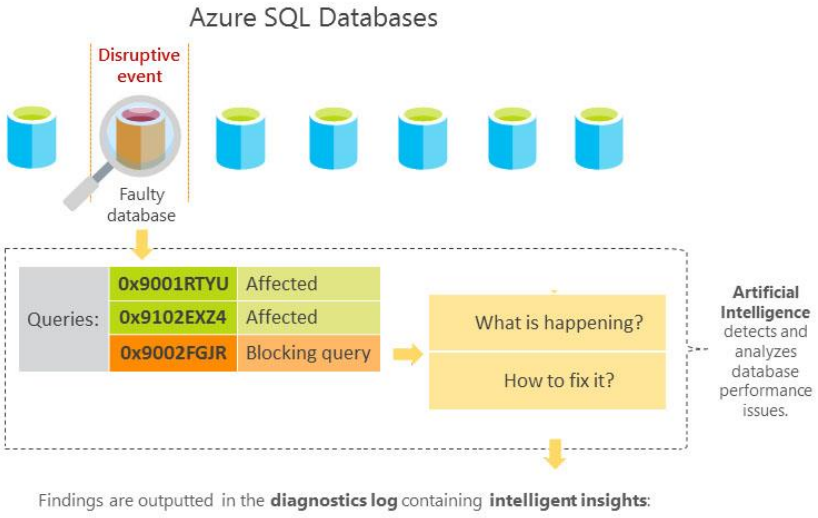


Figura 16 - Detección rápida de errores

2.2. Bases no relacionales

Las bases de datos “no relaciones” o “no SQL” tienen la ventaja de no seguir una estructura debido a que cambian con rapidez, este el motivo que GeoVictoria utiliza este tipo de bases de datos en sus sistemas. Como una base de datos transversal, el uso principal de esta tecnología es albergar los datos que, por su naturaleza, tienen un crecimiento rápido y sin estructura lo que libera a la base de datos principal (la relacional) de almacenar y procesar gran cantidad de registros. Gracias a estos principios se aprovecha la información contenida aquí para el futuro estudio y realización de informes estadísticos y procesos estocásticos (también se les conoce como inteligencia de negocio).
Otro de las funciones que cumple este tipo de base de datos es almacenar datos históricos del cliente. Los que siguen los mismos criterios de seguridad descritos a continuación.
Por último, se almacenan los registros para futuras auditorías y los “logs” de errores y advertencias, tanto de rendimiento como seguridad que posteriormente son notificados a los profesionales encargados por velar por la seguridad y disponibilidad de los datos.

3. Seguridad

Es fundamental para GeoVictoria la confianza con el cliente y por este motivo que aplica el mayor esfuerzo en mantener los datos seguros y disponibles para que el negocio de todos no se vea afectado. Mediante el desarrollo de sistema de encriptación por parte de las aplicaciones y los servicios que Azure entrega el negocio puede funcionar con tranquilidad.

3.1. Encriptación

La primera medida aplicada, a nivel de seguridad por parte de Azure, es cifrar las comunicaciones aplicando TLS/SSL en la capa de transporte. Esto garantiza el cifrado “en tránsito”, entre el cliente y los servidores. TLS proporciona una autenticación sólida, privacidad de mensajes e integridad, interoperabilidad, flexibilidad de algoritmo, y facilidad de implementación y uso. Además, PFS (del inglés Perfect Forward Secrecy) protege las conexiones entre el cliente de los clientes y los servicios en la nube de Microsoft mediante claves únicas. Las conexiones también usan longitudes de clave de cifrado RSA de 2048 bits.
Todas las bases de datos creadas se cifran de forma predeterminada y la clave de cifrado se protege mediante un certificado de servidor integrado. Por otro lado, algunos de los campos más sensibles para los clientes reciben un doble cifrado (números de identificación, números telefónicos, direcciones, contraseñas etc.). Los datos están siempre cifrados, y son descifrados en el momento que las aplicaciones interactúan con la base de datos con Always Encrypted y cifrado de datos transparente.

Always Encrypted permite a los clientes almacenar información confidencial de forma segura fuera de su control directo, es decir en bases de datos de terceros, en este caso GeoVictoria. La información es cifrada desde la aplicación del cliente y almacenada en el motor de base de datos.

El cifrado de datos transparente (TDE) se realiza en tiempo real con una clave de cifrado (clave simétrica AES256) que se almacena en el registro de arranque de base de datos para ser accedida durante la recuperación. TDE protege los archivos de registro y los datos con los algoritmos de cifrado de AES y el estándar de cifrado de datos triple (3DES). El cifrado del archivo de base de datos se realiza en el nivel de página. Las páginas en una base de datos cifrada se cifran antes de que se escriban en disco y se descifran cuando se leen en la memoria.

Por último y no menos importante, GeoVictoria no mostrará a través de sus aplicaciones, datos sensibles de los clientes.

Anualmente, Azure, a través de un organismo de certificación de terceros audita las plataformas que albergan las bases de datos para garantizar el cumplimiento a la norma ISO/IEC 27001 e ISO/IEC 27018.

- Los clientes saben dónde se almacenan sus datos.
- Los datos de los clientes no se utilizarán para fines de marketing o publicitarios sin consentimiento explicito.
- Los clientes saben lo que ocurre con su información de identificación personal.
- Únicamente cumplen las solicitudes vinculadas legalmente para divulgar datos de los clientes.

3.2. Nivel de acceso

Para garantizar la privacidad de los datos de los clientes, GeoVictoria redacta un contrato de confidencialidad entre las partes (entiéndase como las partes el cliente y GeoVictoria).
Los accesos, consultas y modificaciones a los datos son registrados a través de un identificador asignado a cada profesional y queda registrado en un archivo de acceso.

3.3. Roles

Un rol define una serie de permisos y privilegios a un grupo de usuarios para el acceso a los datos. Cada usuario recibe un rol por defecto con accesos mínimos predefinidos para cada ambiente de base de datos. Estos usuarios, con autorización de CISO, CTO y CIO, escalan privilegios en base a las funciones que desempeñan en la empresa. En la siguiente lista se describen los roles existentes:

- **accessAdmin**: Los miembros que pertenecen a este rol definen y modifican los accesos a las bases de datos.
- **ddlAdmin:** Los miembros de este rol pueden definir y modificar estructuras de datos, entiéndase crear, modificar, eliminar base de datos y registros en las tablas.
- **dbBackup:** Los usuarios asignados a este tipo de rol tienen permitido la creación de copias de seguridad de las bases de datos.
- **dataWriter:** Este rol da acceso a los usuarios para agregar, eliminar o modificar datos en todas las tablas.
- **dataReader:** Los miembros de este rol pueden leer datos de todas las tablas de la base de datos.
- **dataDeveloper:** Este rol define los permisos básicos que recibe un profesional por defecto. Estos permisos permiten la lectura y escritura en la base de datos destinada para desarrollo y pruebas.
- **dataProdApp:** Este rol define los permisos básicos que reciben las aplicaciones por defecto. Estos permisos permiten la lectura y escritura en las bases de datos productivas.

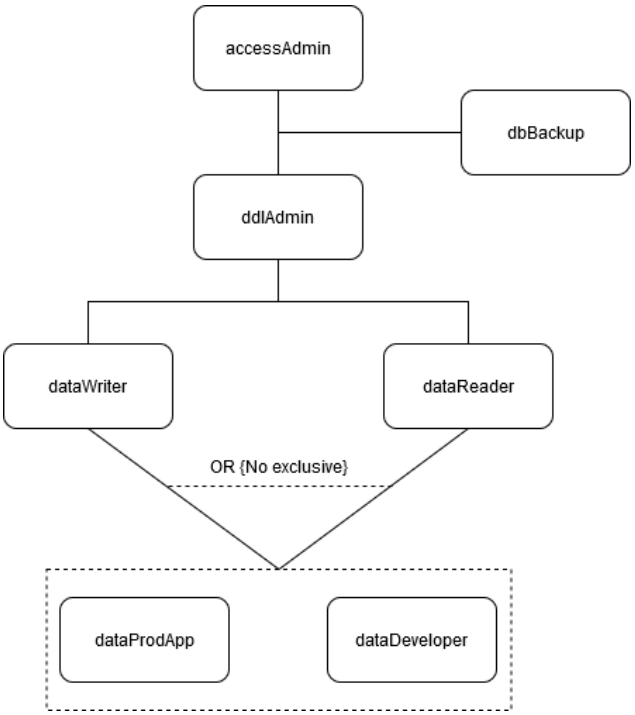


Figura 17 - Jerarquía de roles

3.4. Usuarios

A cada usuario se le asigna un rol, el que es asignado según sus responsabilidades. GeoVictoria diferencia a los siguientes usuarios en el ecosistema de base de datos:

- **Clientes:** Estos usuarios tienen acceso a los datos a través de las aplicaciones y únicamente a la información que estos generan (*revisar acuerdo de confidencialidad*).
- **TI:** Profesionales encargados de desarrollos, mantenciones y pruebas de las aplicaciones de GeoVictoria.
- **BI:** Profesionales enfocados en realizar inteligencia de negocios de los datos.
- **DBA:** Profesionales con la responsabilidad de que los recursos que sustentan y manipulan los datos estén creados, funcionando, optimizados y seguros. A su vez se responsabilizan de la entrega de privilegios a los distintos profesionales.

3.5. Acceso a la información

Gracias al uso de plataformas de servicios de informática en la nube el acceso a los datos está disponible desde cualquier lugar del mundo, lo que da una ventaja cuando se está pensando en una expansión. Con una rápida respuesta por parte del proveedor de servicios en la nube, Azure, su negocio puede seguir funcionando en el lugar que lo necesite.

4. Redundancia de datos

Con el fin de proteger de eventos planeados y no planeados la redundancia de datos juega un papel importante en garantizar la disponibilidad de los datos. Se pueden observar dos grandes grupos que se describen a continuación:

4.1. Contenedor de archivos

- **Almacenamiento con redundancia de zona (ZRS):** Copia de los datos tres veces adentro de una misma ubicación física de la región de Illinois, central norte de Estados Unidos, con una disponibilidad del 99,97% en un tiempo determinado. Este método de almacenamiento es utilizado para dar coherencia, durabilidad y alta disposición a los datos, con una baja latencia, en caso que una determinada región deje de estar disponible.

- **Almacenamiento con redundancia geográfica (GRS):** Copia los datos tres veces adentro de una misma ubicación física de la región de Illinois, central norte de Estados Unidos. Acto seguido, copia de forma asíncrona en una única ubicación física, en la región de Virginia, este de Estados Unidos, a más de 1.000 kilómetros de la región de Illinois, Estados Unidos.

Se debe considerar que los datos replicados en otra región diferente a la principal, están disponibles para su lectura si se habilita dicha opción, para cada cliente, o Microsoft inicia una conmutación por un error inesperado en la primera región.
Como dato importante, al momento de realizar la duplicación de los datos en la región secundaria éstos suelen llevar un desfase de minutos con la escritura en la primera región. Si se produce un error de escritura en la región primaria es muy posible que no se hayan realizado en las demás regiones. Por este motivo que se dispone de información de hora de la última sincronización de todas las operaciones de escritura.

4.2. Base de datos

Azure garantiza una disponibilidad mínima del 99,99% de funcionamiento de la base de datos. Un impacto menor en los mantenimientos e interrupciones programadas y no programadas, actualizaciones, son algunas de las ventajas que la replicación de datos ofrece.
Según el criterio del cliente se disponen de dos versiones de replicación de datos transaccionales:

- **Disponibilidad básica/estándar:** Cuando el flujo de trabajo no se ve afectado en momentos actualización y/o mantenimiento de la base de datos.
  Una capa de proceso se encarga de la instancia del gestor de base de datos en un disco SSD. Este contiene datos transaccionales y almacenamiento en caché, planes de ejecución y búferes. En caso de error, el gestor de instancias, moverá la instancia a otro nodo con capacidad suficiente para llevar a cabo las tareas descritas anteriormente. Los datos no se verán afectados. Se debe tener en cuenta que, teniendo en cuenta que Azure garantiza el 99,99% de disponibilidad, al levantarse una nueva instancia del gestor de base de datos iniciará con la memoria caché vacía y esto podría llevar a experimentar lapsos de demora en la carga y llenado de la memoria.
  La capa de datos se mantendrá intacta, almacenados en un contenedor de archivos con características de redundancia de datos.

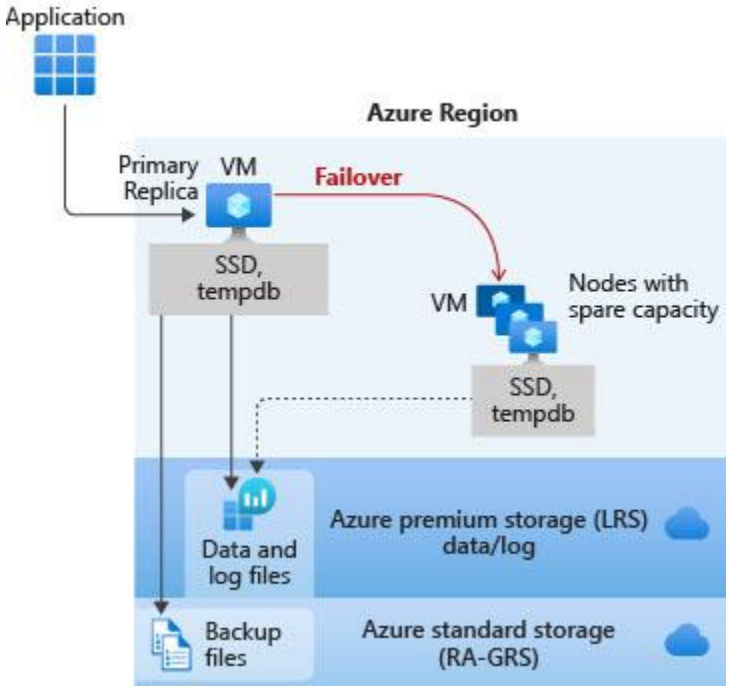


Figura 18 - Disponibilidad básica/estándar

- **Disponibilidad premium/crítica:** Cuando se requiere de un servicio de alta disponibilidad con baja latencia.

Este proceso se lleva a cabo con la creación de un clúster de tres o cuatro nodos que mantiene la instancia del gestor de base de datos. El nodo principal inserta constantemente los cambios en los siguientes nodos y garantizando que los datos se sincronizan con al menos una réplica antes de confirmar la(s) transacciones. En caso de que el nodo principal no responda siempre existe un nodo secundario al que conmutar y actualizado. Cuando vuelve la normalidad en el nodo con error Azure vuelve a redirigir las conexiones al nodo principal.

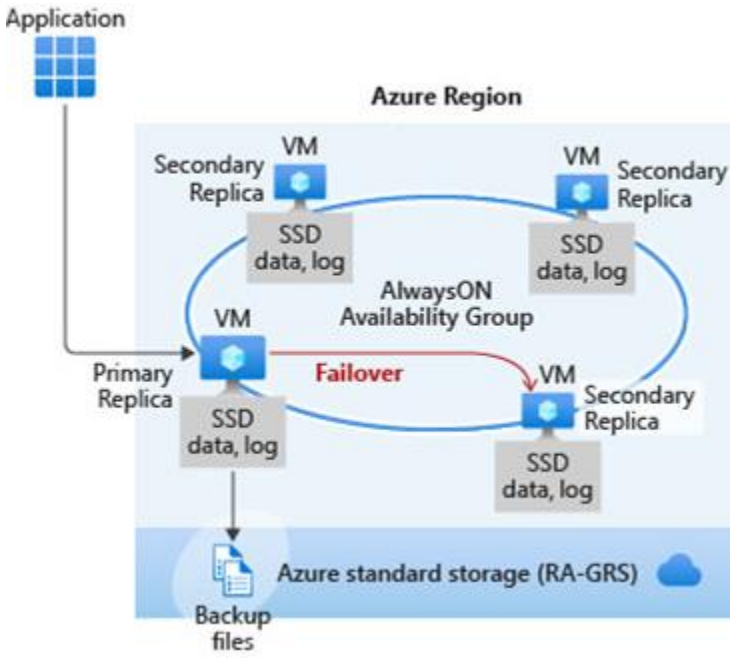


Figura 19 - Disponibilidad premium/crítica

Actualmente GeoVictoria implementa una arquitectura de replicación regional para los nodos de instancia y replicación de datos en diferentes regiones para hacer frente los posibles errores, mantenciones, detenciones planificadas y no planificadas. Además, se implementan balanceadores de carga para dar soporte a un gran número de consulta simultáneas. En caso de producirse un desastre en el centro de datos las instancias seguirán disponibles gracias a la duplicación de los datos.

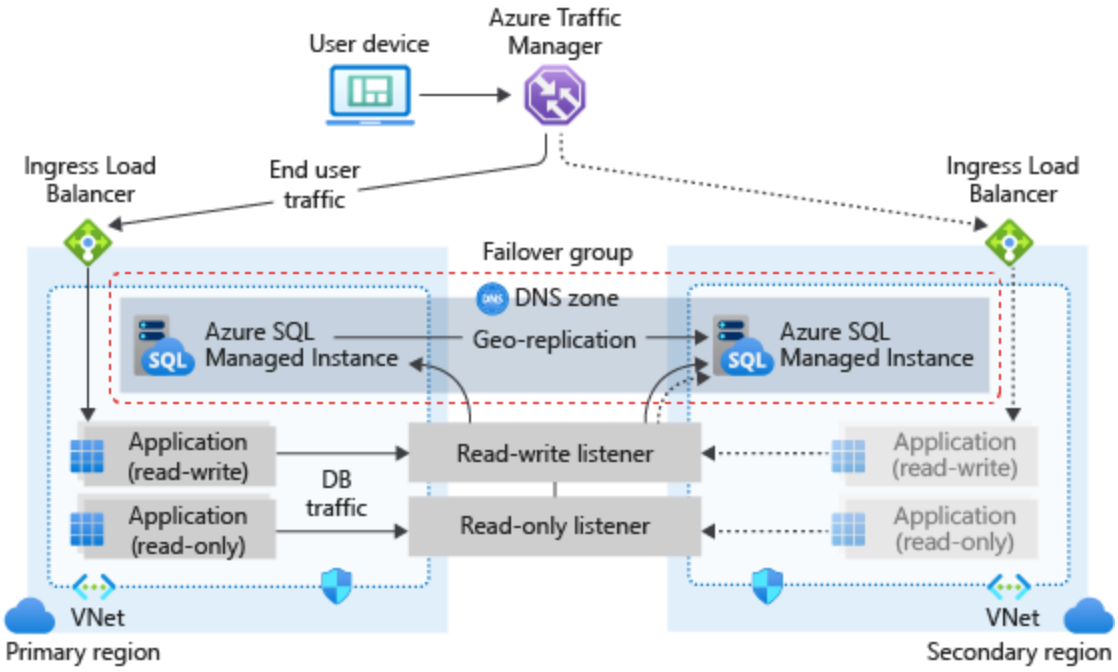


Figura 20 - Replicación de nodos de instancia y datos

5. Proceso de recuperación de datos

GeoVictoria realiza auditorías a los procesos de recuperación de datos en casos de error o catástrofe. Una de las medidas es disponer de una copia física, en posesión de GeoVictoria, de los datos del cliente. Estos son almacenados en plataformas ópticas y resguardadas en un recinto seguro y contra incendios. Por otro lado, se dispone de la arquitectura que entrega Azure SQL Database para la recuperación rápida de datos (ADR) ganando en velocidad sin perder datos. Los procesos de recuperación rápida son muy parecidos a los tradicionales, en los que se cargan las transacciones a través de REDO y UNDO, sin embargo, las operaciones de las transacciones no confirmadas se almacenan en logs (llamados sLogs). En líneas generales, se traduce en versionar las modificaciones físicas de la base de datos, para en el momento que se requiera recuperar una base de datos esta se haga desde el último punto de control y no desde el inicio de la transacción.

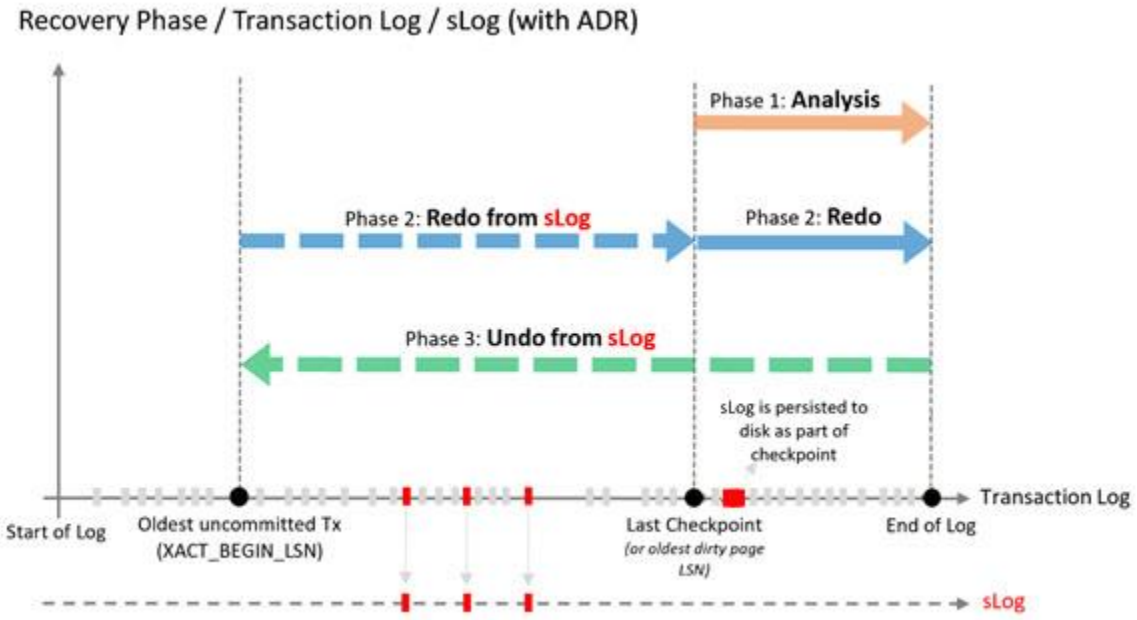


Figura 21 - Proceso de recuperación rápida de datos

6. Tabla de riesgos

La siguiente tabla muestra los tipos de riesgos y las medidas de mitigación para afrontarlos.

Tabla 1 - Riesgos

Nro.	Tipo de riesgo	Descripción del riesgo	Posibilidad	Impacto	Costo	Prioridad
1	Tecnológico.	El sistema no es capaz de obtener datos.	3	10	5	40
2	Tecnológico.	Los datos no están disponibles en la región principal.	3	10	5	40
3	Tecnológico.	Los archivos no están disponibles en la región principal.	2	10	5	45
4	Tecnológico.	La carga de datos se demora.	5	10	5	30
5	Tecnológico.	El cliente no recibe los datos en el tiempo de que necesita.	5	10	5	30
6	Tecnológico.	La aplicación no sincroniza con el servidor.	3	5	2	96

Responsable	Variable de ocurrencia	Mitigación
GeoVictoria	Se reciben llamados de los clientes observando un error en el sistema y no se observan registros de marcas en los horarios punta.	Reporte de estado diario de los servidores en los momentos de mayor tráfico de la aplicación.
Azure	Se reciben llamados de los clientes observando problemas al recuperar los datos. Los sistemas de consulta no responden correctamente.	Disponer de replicación geográfica de datos.
Azure	La descarga de archivos "históricos" no se está pudiendo llevar a cabo.	Disponer de replicación geográfica de archivos.
GeoVictoria	Los resultados de consultas y obtención de datos de la aplicación no son en los tiempos correctos.	Disponer de balanceadores de carga.
GeoVictoria	El cliente argumenta que recibe los datos, pero con demora.	Aumentar plan SQL a premium/Crítico.
Cliente	El colaborador recibe un mensaje de sincronización con el servidor.	Guardar marcas el dispositivo y enviar marcas al obtener cobertura nuevamente.

PROCESO DE DESARROLLO Y GESTIÓN DEL CAMBIO

La forma de llevar control y manejo de proyectos actuales y nuevos dentro de las diferentes plataformas de GeoVictoria, se realiza a través de la metodología DevOps (Development and operation), la que se caracteriza por apuntar a ciclos de desarrollo más cortos que consideran diferentes desarrollos trabajándose en paralelo, sin desmedro de la calidad de los productos finales. Esto se logra a través de automatización de procesos, procesos de mejora continua y colaboración constante de los diferentes equipos del área TI.

Geovictoria se ha enfocado en conseguir un equipo de trabajo cada vez más fortalecido en las políticas de DevOps, dado que aún cuando es una metodología práctica también es un cambio cultural a nivel organizacional. En GeoVictoria se aprovecha el uso de los servicios disponibilizados por Azure y su plataforma Azure DevOps, contando también con un gran equipo de personas certificadas por Microsoft en el uso del mismo.

En esta etapa existen tres roles involucrados:

- Desarrollador
- Team Leader TI
- Jefe de proyecto

1. Términos y definiciones

A continuación, con el fin de establecer un lenguaje común, se detallan algunas definiciones y abreviaturas que se utilizarán en el documento y particular en esta sección.

Sprint: Es un ciclo de trabajo con una duración determinada el cual debe terminar con un entregable a nivel de un proyecto particular.

Feature: Es una pieza de funcionalidad la cual entrega valor agregado al negocio.

Hotfix: Terminología en inglés que significa literalmente “cambio en caliente”, se utiliza para referirse a cambios que deben realizarse directamente en un entorno productivo debido a algún tipo de error en el sistema

Kanban: Es una línea o esquema de producción, en el cual se maneja el avance de cada proyecto en base a pequeñas actividades dentro de una estructura definida. Generalmente las columnas son: To Do, In Progress, Waiting, Done

Branch: Literalmente significa Rama y se refiere a una copia del código de la rama principal. Esta se utiliza para desarrollar nuevas funcionalidades sin afectar el funcionamiento y la consistencia de la rama principal.

Bug: Error en el código debido a problemas de diferente índole.

Pull Request o PR: Es la solicitud de traspaso de los cambios de una Branch de desarrollo a la Branch principal, la cual posteriormente será llevada a un ambiente productivo.

Daily meeting: Reunión de un equipo de trabajo en la cual cada miembro del equipo de trabajo presenta sus avances, además de las complejidades que tuvo o tiene que resolver.

2. Documentación para nuevos Features

En función de explicar principalmente el manejo operativo de GeoVictoria a nivel del departamento de tecnología y desarrollo, será dado especial énfasis a la parte técnica y funcional de la documentación, aún cuando GeoVictoria enfoca todos sus desarrollos en el cliente y la resolución de sus problemáticas operacionales.

En el caso que una empresa requiera nuevas funcionalidades en alguna de las aplicaciones de GeoVictoria, se escribe un documento de requerimientos técnicos por parte del Jefe de Proyecto a cargo de la cuenta. Este documento será posteriormente evaluado por el área técnica, donde el evaluador a cargo levantará los posibles puntos importantes referidos a seguridad de la información, factibilidad a nivel operacional, sistemas de almacenamientos a utilizar y arquitectura del desarrollo, que caso a caso, podrán ser reevaluados por las áreas a cargo de cada uno de estos puntos, para realizar una aproximación correcta de horas de desarrollo que involucrarán

Una vez que el documento pasa las barreras técnicas exigidas por el área y también las necesidades comerciales, se definen los Sprint, tomando en cuenta el correcto orden de los desarrollos definidos dependiendo de la arquitectura de software planteada.

La arquitectura interna de los sistemas de GeoVictoria, así como el trabajo con la metodología DevOps, permite que se pueda realizar desarrollos de diferente índole a la vez para la misma aplicación y manteniendo una mejora continua de los procesos.

Una vez aprobada la documentación para el siguiente sprint, es entregada a las diferentes células de desarrollo. Estás están lideradas por varios Team Leader los cuales manejan la documentación en Work

Items dentro de la plataforma Azure, que permiten llevar control sobre el trabajo de cada uno de estos proyectos.

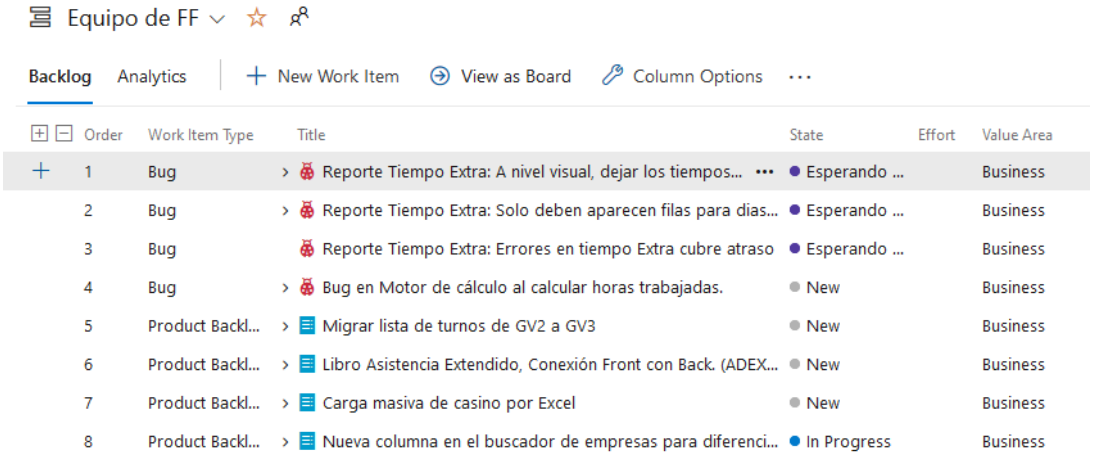


Figura 22 - Work ítems en Azure DevOps

Cada uno de los features o hotfixes se referencian a una iteración de Sprints de una duración de dos semanas. Cada tarea es asignada a cada célula o desarrollador, las que son levantadas como elementos dentro de un Kanban modificable por cada desarrollador, los que a su vez crean pequeñas tareas para conseguir los objetivos presentados en el documento. De esta forma se puede llevar un mejor control de las horas trabajadas para cada objetivo y su cumplimiento. Además, diariamente cada team realiza un Daily meeting, en la cual se señalan los avances realizados el día anterior y en que se trabajará el día actual.

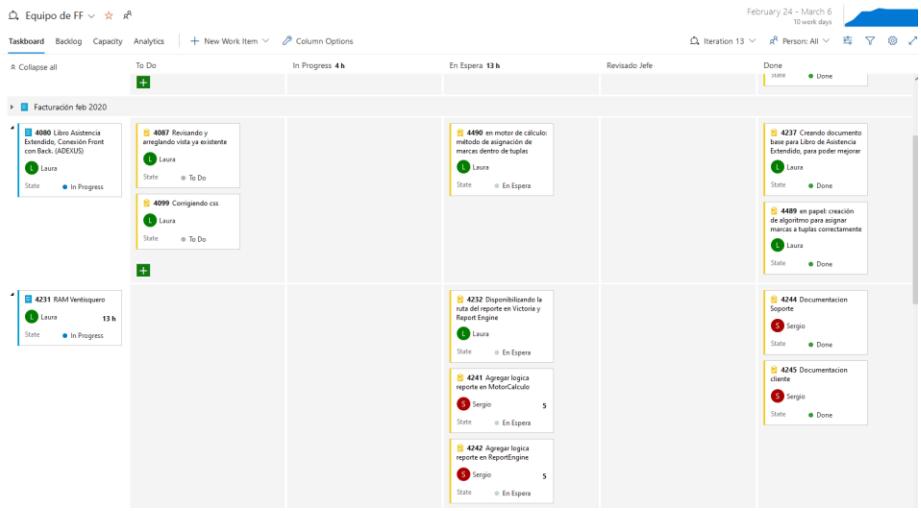


Figura 23 - Vista de Kanban en Azure DevOps

Cada Work item puede ser relacionado con uno o más de estos elementos del Kanban (correlación con cantidad de requerimientos a realizar o bugs encontrados a resolver), estos a su vez van relativos a una Branch nueva que, dependiendo de si es un feature o un hoftix, se saca de la branch Master o Develop, como con el buen uso de Git Flow.

3. Git y manejo de versionamiento

Geovictoria tiene diferentes aplicativos en diferentes lenguajes y frameworks, sin embargo, la metodología de desarrollo esta unificada, de manera de poder llevar de forma certera la mejora continua cada componente.

Todos los desarrollos se guían por una forma limpia de trabajar con GitFlow, teniendo 3 ramas principales de trabajo:

- Master: rama principal de código, en esta rama se mantiene el código productivo de cada una de las componentes del sistema, por lo tanto, a esta rama solo pasa el código de los Features aprobados por el equipo de QA. En el caso de necesitar realizar un Hotfix, la rama base para la codificación de la corrección será la rama Master
- Develop: rama base de desarrollo de software, cada uno de los Features se debe desarrollar en un Branch obtenido a partir de esta rama.
- Release: es una rama obtenida de la rama Develop, la cual es la rama candidata de paso a producción, esta rama debe ser sometida a pruebas por el área de QA para luego ser puesta en la rama master y

llevar a productivo todos los desarrollos que se encuentren completos al final de cada uno de los Sprints de trabajo

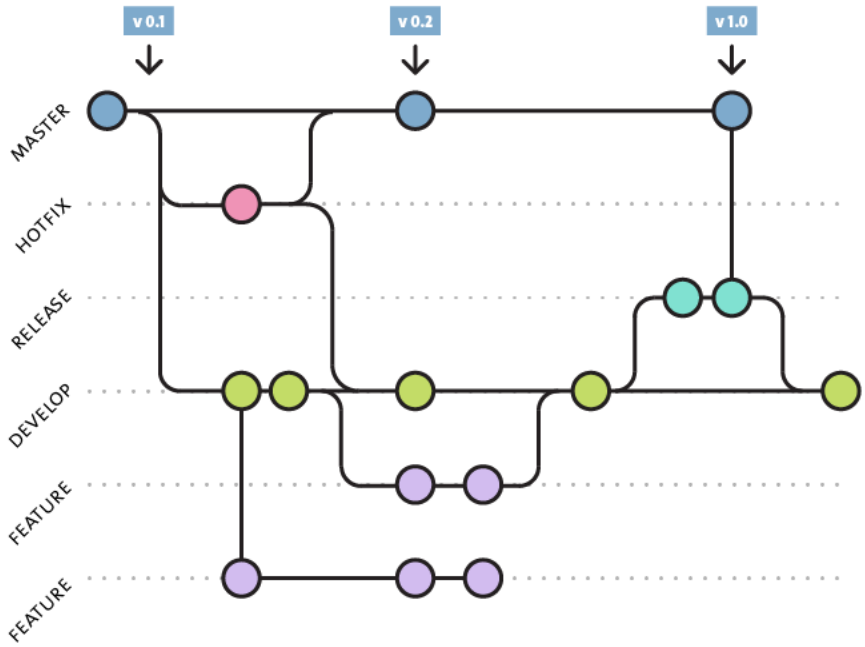


Figura 24 - Diagrama de GitFlow usado por GeoVictoria

Para generar los cambios en las branches correspondientes, se genera un Pull request el cual debe contener un mensaje claro, que refleje los cambios realizados, cada uno de los Pull Request lleva asociado el usuario responsable del mismo, el cual corresponder al usuario que utiliza cada desarrollador en todas las plataformas de Microsoft utilizadas por GeoVictoria.

El proceso de desarrollo implica además que cada Pull Request deben ser revisado en primera instancia por el team leader del equipo en el que se encuentra inserto el desarrollador, este revisará entre otras cosas, el funcionamiento del desarrollo, la arquitectura utilizada en la codificación, el seguimiento de las guidelines de codificación definida, la correcta implementación de los test unitarios que deben estar asociados al desarrollo, etc. Luego de la revisión del Team Leader, el PR pasa a una segunda revisión la cual es realizada por el arquitecto de soluciones a cargo del servicio que el PR este modificando, Luego de que el PR pasa estas dos validaciones, el desarrollo es entregado el área de QA, de manera de que puedan verificar la correctitud del desarrollo en base al plan de pruebas generado según el documento de desarrollo del Feature

Una vez iterado el desarrollo hasta el punto de obtener la aprobación del equipo de QA, la rama en la que este fue desarrollado es integrada a la rama Develop, donde esperará hasta el final del Sprint para ser llevada a producción

Un Pull request también se relaciona directamente con un BackLog Item en Azure DevOPS en donde se encuentra toda la documentación asociada al requerimiento y el proceso de desarrollo del Feature en particular, de esta forma, es sencillo visualizar cada el proceso completa de desarrollo del requerimiento desde una perspectiva global.

En el caso de cambios complejos o muy grandes de la arquitectura interna de alguna aplicación se realiza un Tag en el código, el que permite guardar el último estado antes del paso de este Pull Request a Develop. De esa forma, si este llega a fallar de una forma que no es rápidamente solucionable, el código puede fácilmente volver a la última versión funcional.

Una vez aprobada y generada la versión final para Release, comienza el proceso de publicación.

4. Publicación y procesos automatizados

El proceso de publicación en GeoVictoria se realiza utilizando Pipelines de Azure DevOps, cada uno de los servicios de GeoVictoria tiene asociado y configurado un Pipeline, el cual se encarga de realizar todos los pasos necesarios para una correcta implementación del servicio en Azure, además de esto el Pipeline tiene asociadas todas las variables de configuración necesarias para el funcionamiento del servicio, de manera que la puesta en producción de un servicio no requiere que la persona realiza la publicación conozca cada una de las credenciales de configuración. Existen además pipelines distintos para cada servicio según el entorno en el que se debe realizar la publicación, es decir, para un servicio en particular existe un pipeline para la publicación en QA, uno en Sandbox y otro en Producción, diferenciando en cada caso las credenciales de configuración según ambientes.

Cada una de las publicaciones se realiza sin *downtime*, utilizando el mecanismo de slot diferenciado de Azure, el cual permite realizar dicha publicación en un slot secundario o de stagging, desde el cual se puede intercambiar instancia por instancia hacia el ambiente productivo, de manera que no se produzcan tiempos muertos, además de asegurar que en el caso de que algo estuviese incorrecto en el paso a producción, solo es necesario realizar un intercambio en la dirección contraria de manera de volver a la versión anterior.

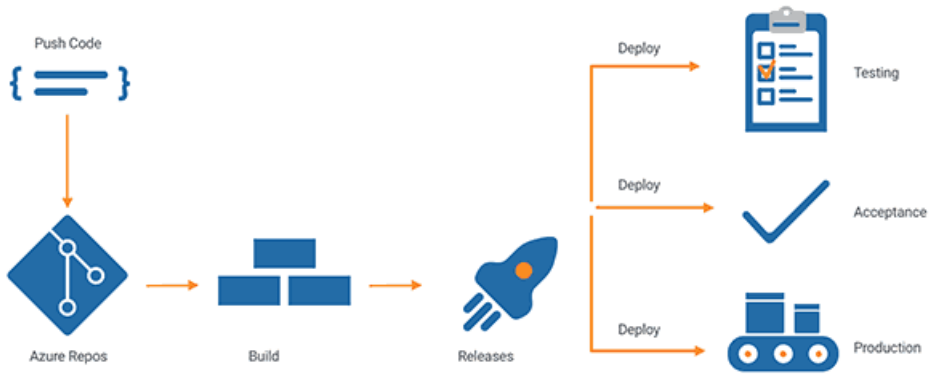


Figura 25 - Diagrama de Azure PipeLines

En la infografía superior se señala la forma en que se planifican los reléase en un pipeline de Azure DevOps, permitiendo automatizar procesos y dejándolos instalados de forma efectiva.

Publicación a Sandbox: La publicación a Sandbox es completamente automática, la aprobación de cualquier PR a la rama Develop gatilla una publicación completa y automática de cada uno de los servicios en el ambiente de Sandbox, esto permite mantener siempre este ambiente completamente actualizado para las pruebas con clientes

Publicación a QA: La publicación al ambiente de QA se gatilla de manera manual por alguno de los Teams Leaders de QA, los pipelines de servicios en este ambiente permiten la selección de que rama en particular se quiere utilizar para la publicación del ambiente de manera de poder probar de forma localizada ciertos cambios importantes.

Publicación a Producción: Luego de finalizado el Sprint, todos los requerimientos finalizados y aprobados por el área de QA son puestos en producción, esta publicación de este pipeline también es gatillado de manera manual, de manera de tener mejor control de la publicación al ambiente productivo final.

5. Grupos y privilegios

Para el correcto funcionamiento del proceso, se requiere que las personas dentro del área de TI tengan acceso a recursos como lo son: códigos de fuente de las aplicaciones, administración de Backlogs Items, administración de Azure Pipelines, etc.

Para esto GeoVictoria genera proyectos en Azure DevOps para cada uno de los servicios que componen su arquitectura completa, estos proyectos contienen los diferentes recursos del proyecto en particular.

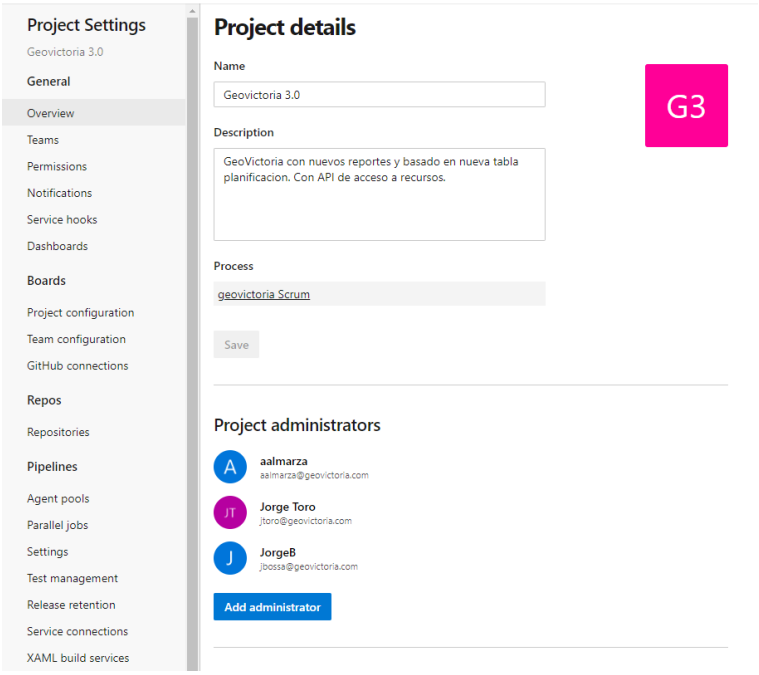


Figura 26 - Ejemplo de proyecto en DevOps

Dentro de cada uno de los proyectos se manejan distintos grupos de usuarios, dentro de estos grupos se configuran los diferentes privilegios que los usuarios pertenecientes a dichos grupos tendrán sobre los recursos del proyecto, esto permite que:

- Cada uno de los desarrolladores de software solo estén añadidos en grupos de proyectos en los cuales se encuentren trabajando, de manera de que el acceso a los recursos no se entregue de manera global
- Entregar accesos que permitan la lectura de ciertos recursos del proyecto sin entregar capacidades de modificación de estos
- Entregar distintos niveles de permios para la aprobación de Pull Request, siendo posible catalogar que grupos deben aprobar antes de seguir avanzando en las fases del desarrollo
- Definir que grupos de usuarios tienen la posibilidad de generar publicaciones utilizando los diferentes Pipelines

Con esto es posible asegurar que la entrega de privilegios a los recursos se realice siempre siguiendo las reglas de privilegio mínimo de manera de que cada persona en la organización solo posea acceso a los recursos que esta necesita para su trabajo diario

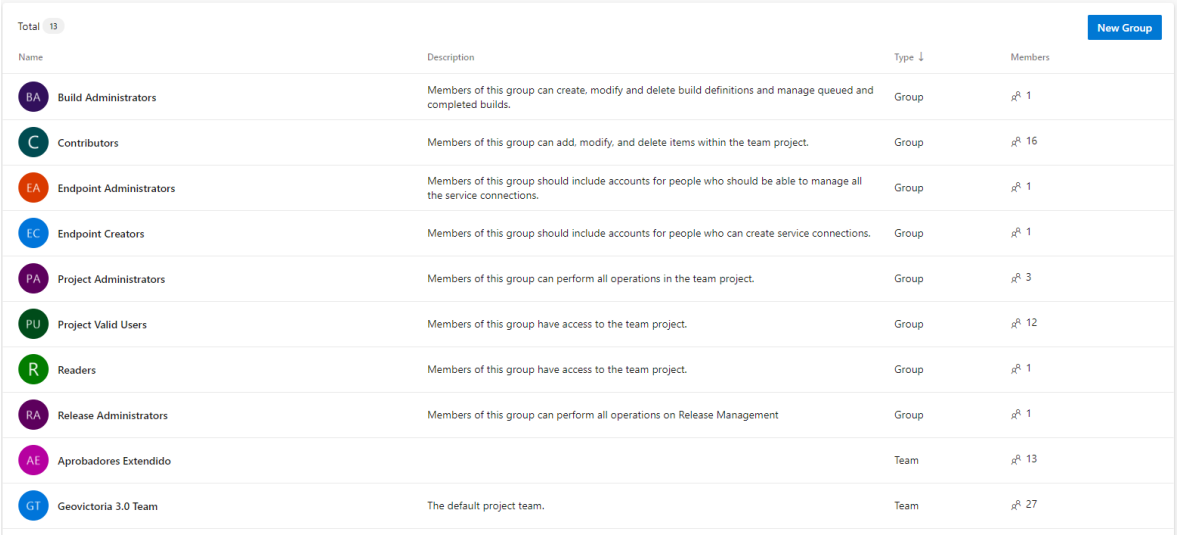


Figura 27 - Ejemplo de Grupos para un proyecto en particular

6. Documentación de entrega de desarrollos

Todos los nuevos desarrollos (Features) contemplados en el nuevo reléase llevan una documentación propia que refiere al uso y funcionalidades de este. Se debe crear un Manual dirigido a el área de Customer Experience GeoVictoria y otro dirigido al Cliente. De esta forma controlamos también el versionamiento de los desarrollos por separado, en el caso en el que futuro se requieran modificaciones en base al funcionamiento de base.

QA & Testing

En GeoVictoria contamos con nuestro equipo de Quallity Assurance (QA) que tiene el objetivo de asegurar el funcionamiento correcto de los desarrollos solicitados antes de su paso a producción y minimizar los errores de cara al cliente, los cuales corresponde tanto a errores lógicos (ie: de código), como errores en la comprensión del requerimiento. Cada desarrollo responde a una serie de requerimientos acordados entre los clientes y los jefes de proyecto. En esta sección se detallará el rol y responsabilidades del equipo para asegurar el funcionamiento correcto del desarrollo. Se describirá el procedimiento a seguir y su ciclo de vida. Esta descripción incluye el estudio de los requerimientos y Casos de Uso, la planificación del testeo, diseño y ejecución hasta el paso del desarrollo a la etapa de release y publicación

En esta etapa existen cinco roles involucrados:

- Team Leader QA
- Tester
- Team Leader TI
- Cliente
- Jefe de proyecto

En donde los primeros tres se involucran de manera más directa con el desarrollo.

1. Terminología y definiciones

A continuación, con el fin de establecer un lenguaje común, se detallan algunas definiciones y abreviaturas que se utilizarán en el documento y particular en esta sección.

Test Plan: Descripción detallada de los objetivos de prueba que se deben alcanzar y los medios y el cronograma para lograrlos, organizados para coordinar las actividades de prueba para algún elemento de prueba o conjunto de elementos de prueba. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Test Suite: Un conjunto de scripts de prueba, Test Cases o procedimientos de prueba que se ejecutarán en una ejecución de prueba específica. [International Software Testing Quallification Board Glossarry]

Test case: conjunto de condiciones previas de casos de prueba, *inputs* (incluidas acciones, cuando corresponda) y resultados esperados, desarrollados para impulsar la ejecución de un elemento de prueba para cumplir con los objetivos, incluida la implementación correcta, identificación de errores, verificación de calidad y otra información valiosa.

Nota 1 a entrada: un caso de prueba es el nivel más bajo de entrada de prueba (es decir, los casos de prueba no están compuestos por casos de prueba) para el subproceso de prueba para el que está destinado.

Nota 2 a la entrada: Las condiciones previas del caso de prueba incluyen: entorno de prueba, datos existentes (por ejemplo, bases de datos), software bajo prueba, hardware, etc.

Nota 3 a la entrada: las entradas son la información de datos utilizada para impulsar la ejecución de la prueba.
Nota 4 a la entrada: Los resultados esperados incluyen criterios de éxito, fallas para verificar, etc. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Resultados esperados: conjunto de resultados esperados a partir de la predicción del comportamiento de los test diseñados basados en los requerimientos del cliente. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Test de regresión: Tipo de testeo que se realiza posterior a las modificaciones para corroborar que cambios realizados en el nuevo Desarrollo no afecten funcionalidades ya existen. [International Software Testing Quallification Board Glossarry]

Testing de caja negra: Tipo de testeo utilizado para probar la funcionalidad del sistema o de una componente sin hacer referencia a la estructura interna. [International Software Testing Quallification Board Glossarry]

Testing de caja blanca: Pruebas basadas en un análisis de la estructura interna del componente o sistema. [International Software Testing Quallification Board Glossarry]

Test Data: Data creada o seleccionada para satisfacer los requerimientos de input para ejecutar uno más casos de prueba, la cual será definida al planificar las pruebas. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Retesting: Ejecución de las pruebas que falló previamente para verificar si las medidas correctivas fueron efectivas. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Resultados de la prueba: Se especifica si la prueba realizada fue exitosa o fracasó y si coincide con el resultado esperado definido. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Ambiente de prueba: Instalaciones, hardware, software, firmware, procedimientos y documentación destinados o utilizados para realizar pruebas de software. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Informe de resumen de prueba: Informe que proporciona un resumen de las pruebas realizadas. [*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

Caso de Uso (CU): Describe detalladamente el requerimiento. Si el *Feature* fuese difícil de manejar (por tamaño, complejidad o cualquier otro motivo) será divido en casos de usos más pequeños. Si el caso de uso proviene de una división, el área de QA deberá informarse del *Feature* completo y los otros casos de uso relacionados, independiente del proceso en el que se encuentren.

Estrategia de prueba: Define las herramientas a utilizar, operatoria (manual o automatizada) o lo que sea necesario para asegurar la consistencia y confiabilidad de la prueba.

Matriz de prueba: Documento que describe los Test cases definidos, su estado, resultado e información asociada a él.

Equipo de Quallity assurance (QA): Equipo que se encarga del testeo de los desarrollos para asegurar su correcta funcionalidad.

Test Unitarios: Un nivel de prueba que se centra en componentes individuales de hardware o software. [International Software Testing Quallification Board Glossarry]

Test funcionales: Pruebas realizadas para evaluar si un componente o sistema satisface los requisitos funcionales. [International Software Testing Quallification Board Glossarry]

Test de Integración: Un nivel de prueba que se centra en las interacciones entre componentes o sistemas. [International Software Testing Quallification Board Glossarry]

Test de sistema: Un nivel de prueba que se centra en verificar que un sistema en su conjunto cumple con los requisitos especificados. [International Software Testing Quallification Board Glossarry]

Testing: conjunto de actividades realizadas para facilitar el descubrimiento y / o la evaluación de las propiedades de uno o más elementos de prueba Nota 1 a la entrada: Las actividades de prueba incluyen actividades de planificación, preparación, ejecución, informes y gestión, en la medida en que estén dirigidas a la prueba. [*International Standard (*ISO/IEC/ IEEE 29119-2), 2013]

Test de aceptación: Pruebas formales con respecto a las necesidades del usuario, los requisitos y los procesos comerciales realizados para determinar si un sistema cumple o no con los criterios de aceptación y para permitir que el usuario, los clientes u otra entidad autorizada determinen si aceptan o no el sistema. [International Software Testing Quallification Board Glossarry]

Niveles de testeo: Instanciación específica de un subproceso de prueba EJEMPLO Los siguientes son niveles de prueba comunes que se pueden instanciar como subprocesos de prueba: prueba de componentes, prueba de integración, prueba de sistema y prueba de aceptación.

Nota 1 a la entrada: Los niveles de prueba también se conocen como fases de prueba.
[*International Standard* (ISO/IEC/ IEEE 29119-2), 2013]

2. Ciclo de vida QA

A continuación, se detalla el ciclo de vida de un desarrollo desde su entrada a esta unidad, hasta su aceptación y publicación.

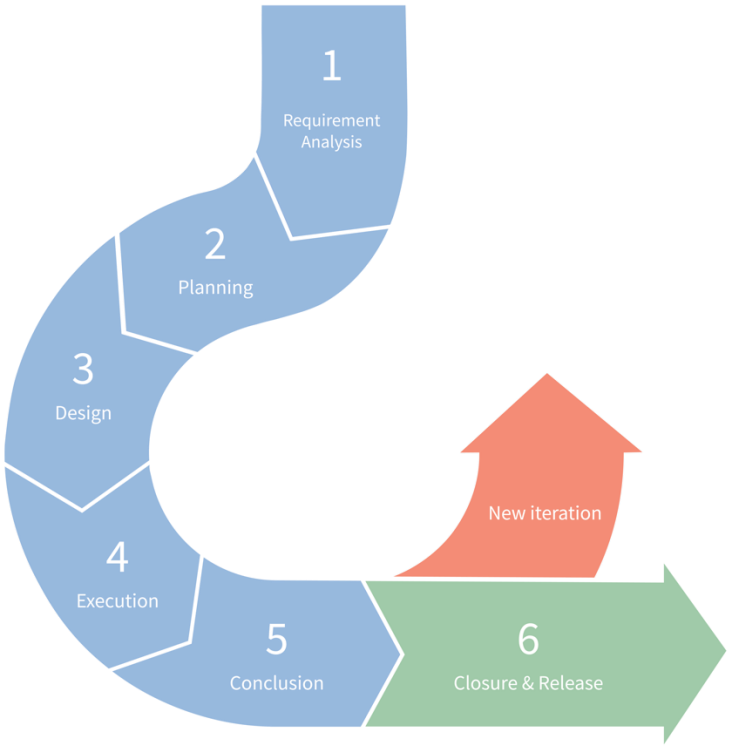


Figura 28 - Ciclo de vida QA

2.1. Estudio de requerimientos

En la primera instancia de un desarrollo, se elabora un documento en el que el cliente especifica los requerimientos de este, los cuales son acordados con el jefe de proyecto. Cada desarrollo debe ser elaborado con el fin de responder a lo solicitado. Paralelamente, este documento es recibido por el equipo de QA, el cual procede al diseño del plan de testeo que se realizará.

En esta etapa del proceso, el Team Leader TI recibe el documento de los requerimientos y CU (Caso de Uso) que dio origen al requerimiento. Se asume que el CU ya fue revisado en una etapa previa (análisis, previo al desarrollo y durante el desarrollo) y por lo tanto es responsabilidad del Team Leader TI la completitud del Caso de Uso. El Team Leader QA tiene por misión entender cabalmente el Caso de Uso, su aplicación en la problemática del cliente y con esa información, disponer del criterio para generar una Matriz de pruebas y una estrategia que resuelva el problema descrito por el cliente
El Tester, deberá –en una reunión con el Team Leader QA - conocer el caso de Uso y validar sus inquietudes o ambigüedades. Posterior a esta etapa se identifican los requerimientos funcionales y no funcionales, elaborando así una estrategia de pruebas la cual, en una última instancia debe ser validada por el Team Leader TI.

2.2. Planificación del testeo

Una vez que hay claridad de los requerimientos a testear y hay una completa comprensión y acuerdo entre los diferentes encargados en el desarrollo, se procede a la etapa de planificación. En esta etapa se definen escenarios prácticos y se genera una Matriz de pruebas (Figura 2). Para poder hacer registro de esta matriz se utiliza la herramienta provista por Azure DevOps Services, la cual facilita la posterior ejecución de los test y estudio de los resultados.

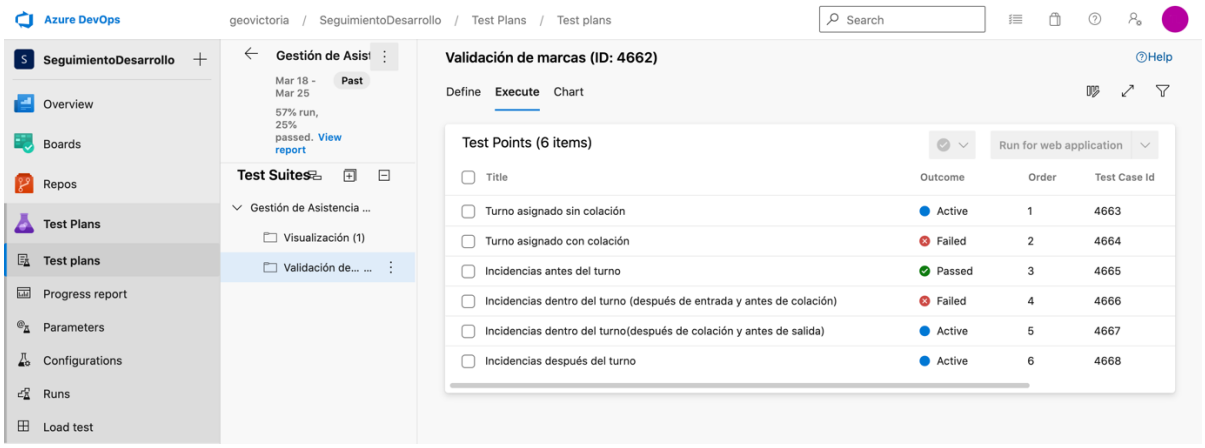


Figura 29 - Ejemplo real de un Test plan e información asociada a su estado.

El Tester, realiza un test plan, el cual esta subdividido en test suites (si corresponde según el requerimiento) y test cases asociados, que permitan validar partes individuales del código. Esta planificación busca cubrir todos los requerimientos solicitados y verificar su correcta funcionalidad como medida preventiva a errores o fallas en la plataforma. En esta planificación, se determinan que test serán ejecutados manualmente o cuales serán automatizados y se define el ambiente prueba para su ejecución.

2.2.1. Test

La planificación de los test tiene el objetivo de cubrir todos los escenarios identificados en la fase de estudio de los requerimientos. En la Figura 3, se muestra los niveles de testeo que se abordan en la planificación. En primer lugar, se inicia con test unitarios, para probar funcionalidades especificas, que siguen normalmente una estrategia de caja blanca y caja negra. Es importante destacar, que los desarrolladores para poder obtener una primera validación su código y para que este sea considerado en esta etapa, debe aprobar con una serie de test unitarios mínimos. Los resultados de estos deben ser reportados junto con evidencia fotográfica al momento de generar el pull request y es un criterio mínimo para que este sea aprobado. Dicho esto, una vez que el Tester define los test unitarios

pertinentes para esta etapa, procede a la planificación de los test funcionales, de integración, de sistema. Este orden permite asegurar la funcionalidad correcta del desarrollo a nivel modular y integrado al sistema original sin perder funcionalidades y detectar errores que puedan impactar las al sistema. Por último, se debe planificar test de aceptación. Estos son de gran relevancia, dado que una vez que el equipo de QA revisa los resultados, si el desarrollo aprueba los test se debe obtener la aceptación por parte del cliente.

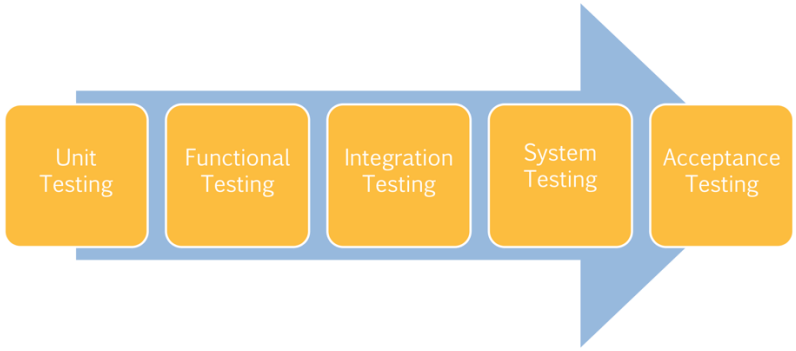


Figura 30 - Niveles de testeo

2.2.2. Ambientes

En GeoVictoria se cuenta con cuatro ambientes principales, el productivo, Sand-Box, de desarrollo y de prueba. El equipo de QA interactúa principalmente con este último. Los desarrolladores trabajan en el ambiente de desarrollo realizando los cambios o adiciones pertinentes para responder a las funcionalidades solicitadas. Una vez el trabajo esté terminado, este debe ser evaluado por el equipo QA antes de pasar a producción.

a. Sandbox

Sandbox es un ambiente en el cual el cliente puede interactuar con las nuevas funcionalidades de la página. De esta manera se puede obtener un feedback directo del cliente y asegurar la calidad óptima del desarrollo que será posteriormente habilitado en producción. Dado que en este ambiente se busca generar una aproximación al cliente lo más cercana a una situación real, la base de datos que se utiliza es una copia a la base de datos de producción que se actualiza periódicamente para asegurar su fiabilidad.

b. Desarrollo

Este ambiente es en el cual se realizan los cambios en el código para poder responder a los requerimientos del cliente. Los desarrolladores al recibir el documento y discutirlo con el Team Leader TI, generan estos cambios. Para poder desarrollar las pruebas pre eliminares utilizan una base de datos poblada que no apunta al ambiente productivo. De esta manera el desarrollador,

puede generar cambios en la base de datos modificando sus atributos y estos cambios no impacten a los clientes.

c. Producción

Este ambiente es con el cual interactúa el cliente, cuenta con los features que ya han aprobado todas las etapas que ponen a prueba su funcionalidad y corroboran que este correcto. Dado que esta es la vista del cliente, en este ambiente se mantiene una versión de la base de los datos actualizada.

d. Ambiente de prueba

Tal como se mencionó anteriormente, en este ambiente es en donde se generan las pruebas. El desarrollo es habilitado en este ambiente el cual apunta al ambiente productivo de Geovictoria. De esta manera se puede simular una situación lo más cercana a la realidad del cliente. Si bien este apunta al productivo, no se utiliza la base de datos del usuario. En la sección siguiente se especifica la elección de la Test Data, su diseño y características.

2.3. Diseño del testeo

Cuando la planificación esté finalizada, esta debe ser aprobado por el Team Leader QA. Este último se encarga de validar la matriz definida, revisar los Test Cases definidos y se valida que la cobertura del testeo cubra todas las funcionalidades y requerimientos solicitados e identificados en la etapa anterior. Si esta planificación es aprobada se procede al diseño de la base de datos (Test Data) que se utilizará para el testeo.

2.3.1. Test Data

Los datos utilizados para realizar las pruebas pueden ser de dos tipos: Datos artificiales que emulen el comportamiento de la empresa o réplicas de los datos reales enmascarados para la protección y seguridad de los usuarios y de la empresa.

En primer lugar, si no es necesario utilizar los datos reales del cliente, se utiliza una base de datos que emule el comportamiento. Se cuenta con una serie de empresas de prueba las cuales difieren en sus características que están pobladas con usuarios, planificaciones turnos, entre otros. Estas son utilizadas principalmente para la realización de prueba funcionales con el fin de replicar escenarios a los que se pueda enfrentar la empresa a través de la página.

Ahora bien, si la funcionalidad a probar corresponde a una nueva configuración en donde los datos utilizados requieren de ser los datos de la empresa, estos deben pasar por un procesamiento para asegurar la privacidad y protección de los datos sensibles. Esta unidad realiza una solicitud de los datos a producción, detallando que características y que datos se requieren. Esta solicitud es documentada

para asegurar un control sobre el flujo de los datos. En este documento se registra la siguiente información

i) Identificador único del documento
ii) Descripción
iii) Responsabilidades
iv) Periodo de uso
v) Confirmación de eliminación

Esta solicitud es procesada y se provee una base de datos con las características solicitadas una vez que esta es procesada, enmascarando los datos sensibles de la empresa tales como los relacionados al usuario y datos previamente acordados con la empresa. Este enmascaramiento se realiza utilizando la herramienta de enmascaramiento dinámico (DDM) habilitada en SQL Server de Microsoft. Es importante destacar, que este equipo no tiene acceso a los datos originales ni permisos para acceder a ella. Una vez finalizada la etapa de testeo, los datos son eliminados y no estarán habilitados para un uso futuro.

2.4. Ejecución de las pruebas

Se ejecutan las pruebas y se registran los resultados obtenidos para cada uno haciendo uso de la matriz diseñada en las primeras etapas del testeo. Además, de ser posible, se registra una evidencia junto a una justificación, lo cual permite también proveer más información al desarrollador ante un eventual rechazo.

2.5. Fase de conclusión

Con los resultados obtenidos en la etapa anterior se genera un documento de resumen con los resultados obtenidos. Utilizando este documento, se determina si se aprobó o no el desarrollo. Si el desarrollo no aprueba alguna de las pruebas diseñadas, se les notifica a los desarrolladores involucrados y se les indica que test falló y la causa. De esta manera ellos podrán realizar los cambios pertinentes, y una vez que finalicen deberán entrar nuevamente en el proceso de QA.

Ahora bien, si el proceso aprueba todos los test diseñados se aprueba el desarrollo por parte del equipo. Sin embargo, esto no implica la aceptación por parte del cliente. En caso de que no se logre la aceptación de parte del cliente, deberá entrar nuevamente al proceso de desarrollo y, por lo tanto, nuevamente a QA, para el cual se hace un *retesting* de todas las pruebas a las que falló y aprobó.

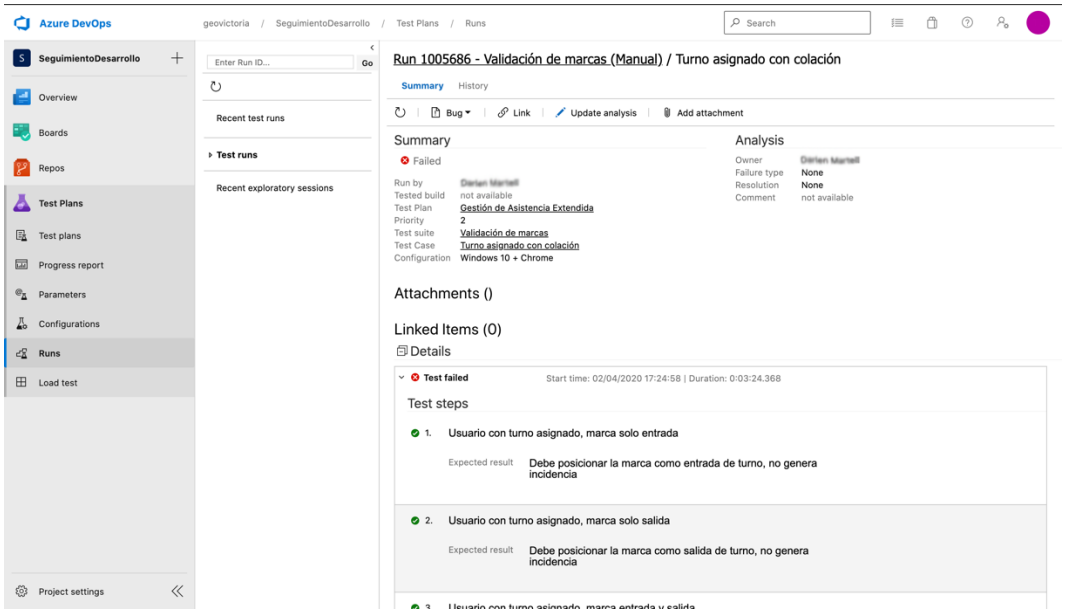


Figura 31: Resumen de uno de los test rechazados

2.6. Fase de cierre y release

Una vez que se ejecutaron y aprobaron las pruebas, y se obtuvo la aprobación del cliente, se pasa a la etapa de cierre y reléase.

Todos los requerimientos que fueron terminados y probados en un sprint en particular son pasados a producción luego de la finalización de este. Este paso a producción se realiza sin *downtime*, utilizando el mecanismo de slot diferenciado de Azure, el cual permite realizar dicha publicación en un slot secundario o de stagging, desde el cual se puede intercambiar instancia por instancia hacia el ambiente productivo, de manera que no se produzcan tiempos muertos, además de asegurar que en el caso de que algo estuviese incorrecto en el paso a producción, solo es necesario realizar un intercambio en la dirección contraria de manera de volver al sitio productivo anterior.

2.6.1. QA Release

Al finalizar el sprint y aprobado todo los tests, el desarrollo este habilitado para su publicación, lo cual se realiza en un “QA de Release”. Esta corresponde a una batería de pruebas integrales las cuales nos permiten asegurar la convivencia de los nuevos desarrollos, entre ellos y contra las funcionalidades existentes. De esta manera se pueden prevenir y anticipar ante posibles errores por compatibilidad que afecten el funcionamiento correcto de la página. En caso de que se detecten errores en esta etapa, estas se realizan en forma de HotFixes al branch candidato a producción (Release Branch), que al igual que todos los desarrollos, deberá entrar en el ciclo de QA y pasar por las etapas de testeo que correspondan.

MANTENIMIENTO DE SOFTWARE

El mantenimiento de una aplicación es crucial para adaptar el negocio al constante y acelerado cambio de las nuevas tecnologías. GeoVictoria cuenta con sistemas y arquitectura para hacer frente a los procesos que conllevan mantener sus aplicaciones actualizadas y con reducción sustancial de errores.

Gracias a un equipo de profesionales, entre ellos arquitectos de software, equipo de aseguramiento de la calidad y desarrolladores, se definen los estándares a cumplir por los servicios de GeoVictoria y se realizan mediciones de las diferentes plataformas periódicamente para cumplir con las expectativas de los clientes. Posterior a la recolección de las mediciones se analizan y se genera un plan de modificaciones en las plataformas para optimizar su eficiencia y reducir los costos operacionales de las mismas.

1. Herramientas de monitoreo

La labor operativa de monitoreo continuo se apoya en herramientas software que facilitan dicha tarea y generan reportes consolidados con información relevante para la toma de decisiones. Las dos herramientas más importantes en los procesos de análisis y detención de errores de las plataformas son:

1.1. Application Insights

Cómo principal herramienta para llevar a cabo el monitoreo se emplea *Application Insights*, herramienta ofrecida por Azure, que recolecta los diferentes eventos del sistema y entrega métricas en tiempo real de lo sucedido en las múltiples instancias de los servicios de GeoVictoria. Con los datos obtenidos de Insights se pueden tomar decisiones de forma rápida y clara para generar una lista priorizada de posibles soluciones. Una de las ventajas de usar *Insights* es la funcionalidad de notificaciones automáticas cuando algunos de los parámetros de calidad establecidos no se cumplen, generando así una notificación oportuna a los responsables de mantener los servicios a punto, cómo lo es el equipo de Continuidad Operativa, y que se genere una reacción inmediata para mitigar el impacto al negocio.

Anteriormente al uso de *Insights* el registro de eventos en los servicios ofrecidos se realizaba a través de la generación de *logs* pero ello derivaba en extensos registros que luego debían ser procesados, en contra al tiempo, para generar datos de estudio. Con la entrada de Insights al ecosistema de GeoVictoria el análisis de logs redujo sustancialmente su dificultad y aumentó su utilidad en la comprensión de eventos que afectan la correcta prestación de los servicios ofrecidos por la empresa.

Una funcionalidad extra y de gran impacto para el negocio que ofrece Insights es el estudio de patrones de uso del cliente para así entender mejor sus necesidades y poderse acercar cada vez más a sus escenarios de uso.

GeoVictoria define estándares de rendimiento para sus aplicaciones (SLA) y junto con el servicio *Application Insights* supervisa periódicamente que dichos estándares se cumplan y entreguen el rendimiento que el cliente espera de los sistemas.

Dentro de la lista de valores informados por *Insights* se encuentran: porcentaje de uso de CPU de cada instancia de servicio, tiempos de respuesta, seguimiento de dependencias, bloqueos de acceso, entre otros. Cuando alguno de estos valores no cumple con el mínimo de servicio establecido se recopila la información y es enviada a los responsables de cada área para su pronto análisis y toma de decisiones.

1.2. Acuetix

Acunetix se presenta como una suite de herramientas automatizadas para verificación de vulnerabilidades de seguridad de los servicios web. Esta herramienta realiza más de 500 tipos de validaciones de seguridad sobre los sitios web de GeoVictoria y sobre el código fuente del mismo aplicando el top 10 de OWASP en cuanto a recomendaciones generadas por dicha organización, tales como inyección de SQL, Cross-Site Scripting (XSS), Insecure Deserializacion, XML External Entities, entre otros. El escaneo periódico se ejecuta sobre todos los sitios web de GeoVictoria en búsqueda de vulnerabilidades.

1.3. Tiempos de mantenimiento

Los tipos de mantenimiento ejecutados en GeoVictoria para garantizar la alta disponibilidad de sus servicios son:

1.3.1. Mantenimiento preventivo

Es un mantenimiento enfocado en mitigar el impacto de posibles problemas que se pueden presentar en los ambientes de ejecución productivos de los servicios, bien sean problemas producidos por configuraciones del ambiente o por errores internos de la aplicación desarrollada, previene de la aparición de posibles errores que puedan surgir en el futuro cercano y lejano.

Anualmente, con el apoyo de una empresa externa de seguridad, se ejecutan pruebas y se analizan resultados de todos los *endpoints* públicos de los servicios habilitados. El informe de la empresa

externa se interioriza y basado en ello se genera un plan de correcciones y nuevamente de validaciones de los canales de conexión.

Por otra parte, las bases de datos son accedidas por el equipo de ingenieros de GeoVictoria, con roles y permisos adecuados, para realizar una reconstrucción de los índices de las tablas y realizar pruebas de recuperación de los datos con periodicidad mensual, estas pruebas son realizadas en ambiente de pruebas sin afectar a los ambientes productivos, todo acorde con el plan de recuperación de desastres - DRP. Los datos recolectados de estas pruebas periódicas generan informes usados posteriormente para derivar en la toma de decisiones y consecuentemente en la actualización de la arquitectura de la solución y de los procedimientos establecidos.

Respecto al código fuente, el uso de herramientas como Acunetix, pruebas unitarias, Azure DevOps, *Application Insights* y otras, ayudan a los profesionales de GeoVictoria a anticiparse a la aparición de errores y mejoras para el cliente. Además, se recogen los patrones de uso de la plataforma que permite realizar cambios favorables en el uso diario.

Mensualmente se realiza un informe que alimenta las mediciones de desempeño (KPI) de la empresa y genera mejoras en las operaciones diarias. Estos informes son registrados en *logs* que alimentan la plataforma de *Microsoft Power BI* que permite dar un vista general y simplificada de la información para que sea humanamente entendible y útil. El análisis de efectividad de los equipos de trabajo inicia desde el nivel táctico de la empresa y se ramifican en cada una de las áreas del nivel operativo.

1.3.2. Mantenimiento predictivo

Haciendo uso de los servicios de Azure se tiene conocimiento de los índices de consumo de CPU, memoria, número de conexiones entrantes, tiempo de respuesta y otros parámetros y, gracias a estos servicios, GeoVictoria se anticipa a la ocurrencia de un posible fallo en las diferentes plataformas, basándose en las métricas de estado.

Los algoritmos utilizados se basan en los datos recopilados por diversas herramientas de monitoreo: *Panotpta*, *Kingdom*, *PingDom* y *Azure Application Insights*. La diferencia entre el estado esperado y el estado actual de la plataforma es notificada a los equipos de ingeniería de las áreas con información de los eventos acontecidos para identificar y anticiparse a las intervenciones de un mantenimiento más profundo que puedan afectar al cliente.

GeoVictoria aprovecha la tecnología *serverless* para fragmentar en unidades más pequeñas las diferentes tareas que los sistemas realizan en servicios y así minimizar los riesgos que conlleva

realizar un mantenimiento correctivo generado con escasez de tiempo. El equipo de aseguramiento de la calidad realiza pruebas y análisis diarios de las métricas que las diferentes plataformas entregan para generar cambios y, en consecuencia, optimizaciones al sistema.

Cuando existe un evento disruptivo, gracias a los datos obtenidos de las plataformas de análisis y diagnóstico, se reúne al personal de las diferentes áreas se da solución al evento disruptivo cómo se plantea en el plan de continuidad del negocio. Esto puede traducirse en aumento de las capacidades de los servicios en Microsoft Azure y/o actualizaciones de las parametrizaciones de escalabilidad de los mismos para dar solución inmediata y a largo plazo del problema encontrado.

Los datos recopilados en estos procesos son almacenados para su futuro estudio en las reuniones mensuales de operatividad de la plataforma y valores estadísticos que alimentan, de forma retroactiva, la realización de un buen mantenimiento preventivo.

1.3.3. Mantenimiento correctivo

Al presentarse un evento disruptivo que amenace la correcta operación de uno o varios servicios se inicia diagnosticando el error, entendiendo su naturaleza y el por qué se produce. Para lograr este entendimiento del problema GeoVictoria hace uso de las herramientas de las que dispone para recopilar información tal como la procedencia del error, la fecha y hora del suceso, el tiempo que duró, el causante de éste, el cliente que sufrió las consecuencias, entre otros aspectos.

Acto seguido, los equipos de trabajo de cada área involucrada reciben la información e inician una investigación para luego informar al área de aseguramiento de calidad (QA) para que ejecuten las pruebas de verificación y tratar de reproducir el escenario de fallo.

Es importante mencionar la importancia de la participación del área de soporte en estos casos dado que ellos pueden tener información sobre errores similares o aquellos que el cliente haya reportado con anterioridad relacionados, de esa forma se recopilan más antecedentes para tomar una buena decisión al respecto. El área de soporte presta servicio como apoyo al cliente ante posibles eventualidades, dudas del cliente en el uso de la plataforma o errores presentados, para posteriormente ser registrados en *tickets* que se escalan hasta un nivel de servicio 3, en la medida que el grado de complejidad del error lo requiera.

Por otra parte, los errores que puedan surgir son caso de estudio gracias la arquitectura de aprendizaje creada en Azure. Esta plataforma recibe los errores de las diferentes aplicaciones para ser procesadas por una serie de nodos expertos que alimentan una base de datos de estudio. Posteriormente, y de forma semanal, un equipo de profesionales del área de aseguramiento de la

calidad realiza reuniones para estudiar los casos y plantear posibles mejoras para prevenir nuevos errores y generar estadísticas que conllevan a mejoras en los sistemas.

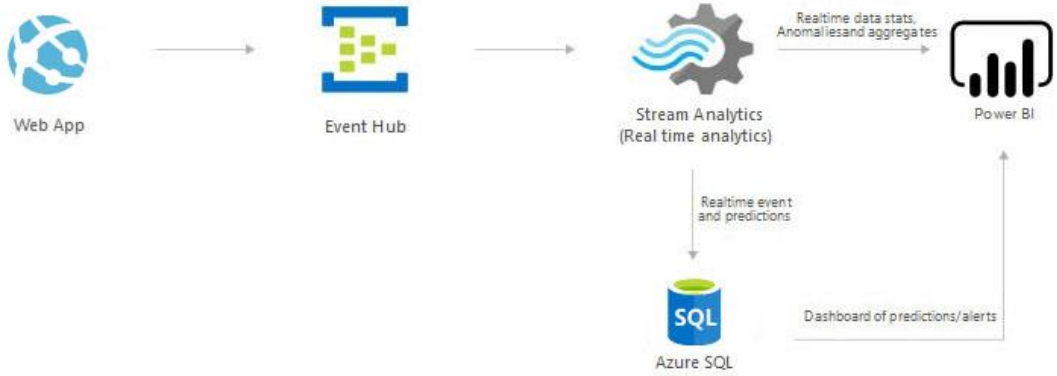


Figura 32 - Ciclo de aprendizaje de errores

1.3.4. Mantenimiento perfectivo

En GeoVictoria, existe un equipo de arquitectura y una división encargada del estudio constante de los sistemas y aplicaciones. Este equipo analiza las tendencias del mercado y futuros cambios que afectarán al medio ambiente en los que las aplicaciones se desenvuelven, un ejemplo de ellos es el constante cambio en el mundo de los navegadores web. El equipo analiza, a través de la documentación de los sitios oficiales, los cambios que serán añadidos a futuras versiones y genera documentos de cambio favoreciendo la evolución de las aplicaciones y mitigando la posibilidad de que se presenten errores de adaptación al medio. Gracias a que GeoVictoria es *partner Gold* de Microsoft, las pruebas se realizan sobre las versiones beta de los productos Microsoft antes de que sean comercializadas al mundo entero y adelantarse así a los posibles errores por actualización tecnológica.

Existe una serie de pasos a seguir para la comprensión de los cambios a realizar:

1. Este primer paso emplea el 50% del tiempo del mantenimiento. El equipo obtiene en éste paso el conocimiento que el cambio implica, valor agregado para el cliente, tiempos de inactividad y su mitigación, los sistemas afectados y riesgos asociados. También se realizan pruebas en ambientes previos dispuestos para tal efecto, para ejecutar pruebas automatizadas y heurísticas.
2. Recopilar la información y realizar la mejora dada en el sistema. Las mejoras pueden enfocarse en áreas específicas como, por ejemplo, estructuras de datos, lógica del proceso, interfaces y documentación. GeoVictoria fragmenta dichas modificaciones para evitar que éstas tomen más de un cuarto del tiempo total del mantenimiento.
3. Por último, se realizan las pruebas que aseguren la calidad y el mantenimiento de los estándares mínimos de calidad que GeoVictoria debe garantiza en sus nuevos desarrollos o cambios de

parametrización de los ambientes de ejecución. El área de aseguramiento de la calidad, aplicando el estándar ISO/IEC 25000 SQuaRE y contando con profesionales con certificaciones ISTQB, ejecuta pruebas de rendimiento, pruebas de estrés, seguridad y heurísticas en toda modificación o nueva funcionalidad que se vaya a publicar para cumplir con los requisitos y el estándar que exige GeoVictoria.

GESTION DE INICIDENCIAS

GeoVictoria posee diversos mecanismos de monitoreo y levantamiento de alertas. Estas cumplen el rol de asegurar un funcionamiento correcto de la página y notificar lo antes posibles errores que deban ser corregidos.

1. Roles

Los principales roles que interactúan en este proceso se presentan a continuación. Cada uno de ellos cumple un rol específico desde la detección de la incidencia hasta la aprobación de la corrección.

- Equipo de Seguridad
- Equipo de desarrollo
- Equipo de Customer Success
- Cliente
- Equipo de Continuidad Operativa
- Equipo de Custumer Experience
-

En las siguientes secciones se detalla que actividades realiza cada uno y como interactúan entre ellos.

2. Flujo gestión de incidencias

A continuación, se describe el flujo de gestión de incidencias. Este corresponde al protocolo que se utiliza para la resolución de una incidencia. Se describe desde el levantamiento de la alerta hasta la publicación y aprobación de la solución diseñada.

2.1. Recepción de alertas

El proceso comienza con la recepción de alertas. Estas pueden provenir de dos fuentes en particular. La primera, de manera externa, a través de una alerta levantada por el cliente y la segunda, por monitores internos detectados por el equipo de Customer Service.

2.1.1. Incidencias detectadas por el cliente

El cliente al interactuar con la plataforma podría detectar algún problema o error que esté afectando el funcionamiento correcto de alguna sección del servicio, en el caso de que esto suceda, el cliente puede

notificarlo a GeoVictoria a través del envió de un ticket a la mesa de ayuda. En este ticket el cliente describe el problema el cual deberá ser validado para así comenzar el proceso de gestión de incidencias.

Este ticket es recibido en una primera instancia por el equipo de Customer Experience. El cual se encarga de revisar la alerta levantada por parte del cliente y estudia el incidente. Tras esta revisión si el equipo logra detectar el origen del problema y tiene las herramientas para proporcionar la solución, le indican la información de corrección del incidente al cliente, ya que en este caso lo más probable es que se deba a un error de configuración o manipulación de la plataforma.

Si el equipo no logra identificar la causa de la incidencia, el ticket escala al equipo de Continuidad Operativa y se informa al cliente del avance ticket en el flujo.

2.1.2. Procesos de monitoreo interno

Nuestras áreas de Customer Experience y Desarrollo, poseen herramientas de monitoreo tanto manuales como automáticas, estas, permiten conocer el estado y funcionamiento del servicio. A través de estas herramientas monitorean la página y pueden detectar incidencias en él. Al detectar cualquier tipo de incidencia o deterioro de los servicios se levanta una alerta la cual será recibida por el equipo de Continuidad Operativa.

2.2. Clasificación de incidencias

El equipo de Continuidad Operativa recibe la descripción de la incidencia detectada. Ellos se encargan de revisar y entender cuáles son los riesgos, los servicios impactados y a los clientes involucrados. En caso de que se identifique que hay más de un cliente involucrado estos son informados de la situación y se les informará cada una hora por medio de reportes el progreso y estado de la incidencia.

A partir de este análisis se realiza una clasificación, la cual depende del impacto que está teniendo sobre la página, la cantidad de clientes y la urgencia que tiene la resolución del problema particular. Para poder realizar esta clasificación se estudian estas variables y se posiciona la incidencia en el cuadrante correspondiente. Como se muestra en la Figura 3 una incidencia que se identifica como urgente y que tienen un mayor impacto tendrá una mayor prioridad, al caer en el cuadrante de prioridad 1. Dentro de esta categoría se ubican, por ejemplo, fallas en marcaje o problemas al cargar la página y en general aquellas funcionalidades que inhabilitan de forma crítica el funcionamiento de la plataforma. Mientras que incidencias de baja prioridad son aquellas de bajo impacto y urgencia, como por ejemplo errores en la terminología utilizada en las vistas de la página web o bugs de menor importancia para el funcionamiento global de la página. Este criterio permite generar un orden y administrar de mejor manera los errores que se vayan detectando.

Una vez realizada la clasificación el equipo de Continuidad puede determinar la complejidad y que tan crítica es la incidencia identificada. Este equipo cuenta con herramientas personalizadas de GeoVictoria para la corrección de problemas comunes. Si la incidencia identificada no es crítica y se identifica como común, este equipo es el encargado de solucionarlo y notificar a Customer Experience para que se comunique con el cliente y le notifique del nuevo estado de su alerta.

Ahora bien, si la incidencia no puede ser resuelta con estas herramientas entonces se deriva a el Equipo de Seguridad.

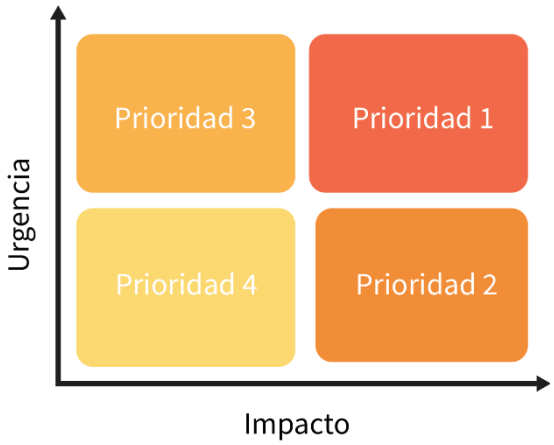


Figura 33 - Criterio de clasificación.

2.3. Derivación a Equipo de Seguridad

El equipo de Seguridad se hace cargo de las incidencias que se escapan de poder ser solucionadas con las herramientas previstas por el equipo de Continuidad. En primer lugar, a los clientes involucrados se les notifica del nuevo estado en el que se encuentra la incidencia. En segundo lugar, se genera un Documento de Problemas e Impactos. En este documento se registra; fecha de recepción, descripción de la incidencia y clasificación. Este documento es enviado a el equipo de QA que realiza el levantamiento del plan de mitigación y corrección de la incidencia.

2.4. Reproducción de la incidencia

El equipo de Continuidad se encarga de enviar el documento generado al equipo de QA. Este equipo estudia el caso y prioriza el estudio según el grado de importancia que se haya identificado. Este equipo se encarga de reproducir el problema, encontrando las secciones particulares del sistema que se encuentra involucradas y que requerirán de posibles modificaciones.

Con esta información, se genera un reporte en donde se especifica la información obtenida que será puesta a disposición del equipo de Desarrollo. Paralelamente, genera un plan de pruebas que posteriormente se utilizará para el testeo de la funcionalidad.

2.5. Desarrollo de la solución

Como se mencionó en la sección anterior, el equipo de Desarrollo recibe un reporte por parte del equipo de QA. En donde se identificó a nivel de implementación la incidencia reportada. Este equipo se encarga de identificar el bug y corregirlo realizando las modificaciones en el código que solucionen el problema.

Además, en caso de que sea necesario se encarga también de iniciar mecanismos de recuperación en caso de que la incidencia sea generalizada o afecte las bases de nuestro servicio.

Al completar el desarrollo, se procede a la realización de un Pull Request, para que sea revisado, por los agentes involucrados en los servicios afectados por la incidencia.

2.6. Quality Assurance y testeo de la funcionalidad

Para asegurar el funcionamiento correcto de desarrollo implementado el equipo de QA implementa una serie de pruebas sobre ella. Utilizando el plan de pruebas diseñado en la etapa previa, revisa que la corrección del bug sea correcta. En caso de no estarlo, se deriva nuevamente al equipo de Desarrollo, que deberá iterar sobre el código y volver a realizar los cambios que correspondan. Si la funcionalidad esta correcta, se le notifica al equipo de Seguridad.

El proceso de QA & Testing se muestra con mayor detalle en su sección respectiva, en donde se describe de manera detallada sobre el proceso de flujo y ciclo de vida de un desarrollo que entra a esta unidad hasta que es publicado en producción.

2.7. Revisión funcional

Una vez que la solución fue publicada en producción se le notifica al equipo de Seguridad. Este equipo se encarga de revisar la funcionalidad nuevamente en producción. De esta manera se asegura que la funcionalidad afectada y notificada por el cliente haya sido correctamente solucionada. Si la solución no es correcta se le notifica al equipo de QA, el cual deberá nuevamente revisar el error, realizar un plan de pruebas y comunicarle al equipo de desarrollo sobre la nueva solicitud. En el caso contrario, en el que la solución es correcta, se le notifica al equipo de Customer Experience que la incidencia fue corregida.

2.8. Notificación a clientes

Al recibir la información por parte del equipo de Seguridad, que la funcionalidad fue corregida, el equipo de Customer Experience se encarga de notificar al cliente la completitud de su solicitud.

2.9. Monitoreo de la solución

Por último, la solución es monitoreada por el equipo de Customer Experience. Este equipo monitorea el estado del servicio y de la nueva solución para asegurar la efectividad y satisfacción del cliente.

A modo de resumen, en la Figura 1, se presenta el flujo de gestión de incidencia cuando la alerta levantada fue por parte del usuario. Mientras que en la Figura 2, se muestra el flujo correspondiente a una levantada por el equipo de Customer Experience.

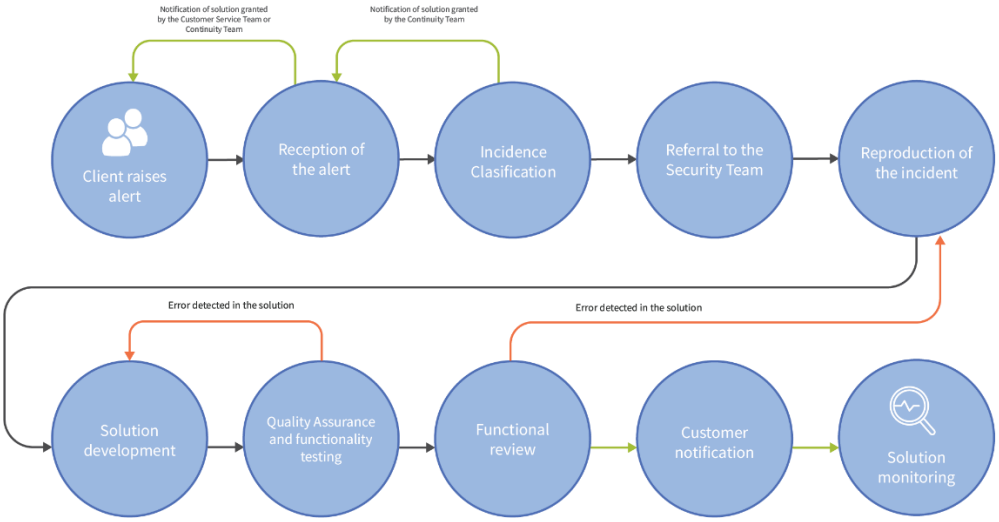


Figura 34 - Flujo de gestión de incidencia para clientes

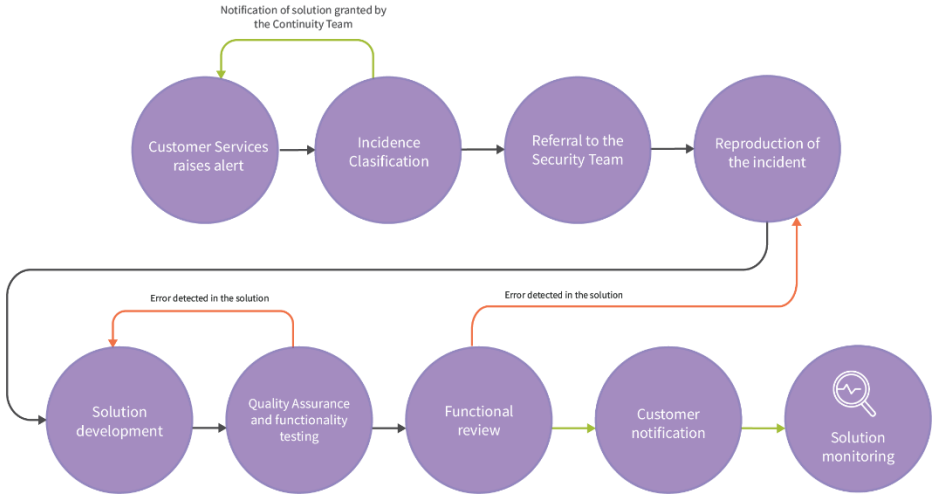


Figura 35 - Flujo de gestión de incidencia para alerta levantada por el equipo de Customer Experience

3. Procedimientos periódicos

GeoVictoria realiza procedimientos periódicos de análisis de código y posibles vulnerabilidades técnicas sobre los componentes del servicio, estos procedimientos se pueden separar en dos tipos:

- Procedimientos internos: Mensualmente el equipo de seguridad realiza un escaneo de vulnerabilidades, utilizando el software Acunetix, dicho software entrega una serie de incidencias que afectan a cada uno de los endpoints disponibles del sistema en su totalidad

- Procedimientos externos: Cada seis meses, se realiza un proceso de Hacking Ético, a cargo de una empresa externa, este procedimiento se hace utilizando metodología de caja negra, levantando así las posibles vulnerabilidades que posee nuestra plataforma web.

3.1. Corrección de vulnerabilidades

En el momento de que alguno de los procedimientos periódicos es llevado a cabo, se obtendrán una serie de vulnerabilidades que deben ser atacadas de manera de reducir todos los posibles riesgos que estas vulnerabilidades generen, para esto se asignan dos equipos de trabajo, un equipo de trabajo del área de QA el cual se encarga del levantamiento, reproducción y gestión del plan de pruebas y un equipo de desarrollo, el cual se encarga de la corrección a nivel de código de las vulnerabilidades encontradas. Estos equipos se encargan exclusivamente de la corrección de estas incidencias hasta que estas se encuentren corregidas a cabalidad.

El tamaño de los equipos encargados de las correcciones varía de acuerdo con la cantidad y criticidad de las vulnerabilidades encontradas, en el sentido de que el equipo requerirá más personas en el caso de que las vulnerabilidades sean críticas o que existan una gran cantidad de vulnerabilidades, además de esto el tamaño del equipo puede cambiar a medida que las vulnerabilidades críticas se van corrigiendo.

PLAN DE RECUPERACIÓN DE DESASTRES - DRP

Los desastres están presentes en la vida cotidiana y nunca la probabilidad de que ocurran es cero, por lo tanto, toda empresa debe estar preparada para afrontar de manera adecuada los posibles desastres que la puedan afectar con análisis, planeación, pruebas continuas y actualización de los planes de manera que al presentarse un evento de riesgo la operación no se vea afectada o que el impacto sea lo mínimo posible.

Por todo lo anterior surge la necesidad de generar e implementar el Plan de Recuperación de Desastres para GeoVictoria que permita garantizar la restauración en corto tiempo de las operaciones esenciales, de una correcta implementación de este plan depende el impacto de un evento de riesgo para GeoVictoria y sus clientes.

1. Terminos y definiciones

Con el fin de establecer un lenguaje común y claro se dan algunas definiciones y abreviaturas que tendrán lugar en el presente documento.

Actividades prioritarias: Aquellas actividades que tomar la mayor prioridad en caso de un evento de riesgo con el objetivo de mitigar el impacto a la operación.

Amenaza: Percepción de la posibilidad de ocurrencia de algún hecho dañino sobre los recursos involucrados en el desarrollo de un proceso (humano, financiero, medio ambiente, información e imagen corporativa), representando pérdidas para el sistema o la organización. [*International Glossary of Reslience*].

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. Este análisis permite evaluar el riesgo y la estimación del mismo. [Norma ISO 31000:2011, Capitulo 2, Términos y definiciones, numeral 2.21].

Análisis de impacto al negocio (*Business Impact Analisys* - BIA): Refiere al documento que identifica de forma clara la disponibilidad que se requiere de la plataforma tecnológica para soportar los procesos de la entidad para garantizar la continuidad del negocio y la prestación del servicio a los clientes.

Árbol de llamadas: Documento que describe gráficamente las responsabilidades y el orden en que deben producirse las llamadas a los diferentes niveles de la organización, así como a los clientes y

proveedores y otros contactos clave en caso que se produzca una emergencia, catástrofe o situación de indisponibilidad grave. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Centro de operaciones de emergencia (COE) (sala de crisis): La ubicación física y/o virtual desde donde se toman las decisiones estratégicas y se dirigen, coordinan y monitorean todas las actividades de un evento/incidente/crisis. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Centro Alterno de Procesamiento de Datos (CAPD): Lugar en donde se ejecutan los procesos informáticos de una empresa cuando no es posible hacerlo en el CPD.

Centro de Procesamiento de Datos (CPD): Lugar en donde se ejecutan los procesos informáticos de una empresa necesarios para la prestación del servicio a sus clientes.

Continuidad del Negocio (CN): Capacidad de la organización para continuar con la entrega de sus productos o servicios a niveles aceptables predefinidos luego de un incidente disruptivo. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.3]

Crisis: Situación anormal e inestable que amenaza los objetivos estratégicos, la reputación o la viabilidad de una organización. [BS 11200:2014 – *Crisis Management – Guiadance and good practice*, Capitulo 2, Términos y definiciones]

Desastre: Un evento repentino, no planeado y que pone en peligro la capacidad de una organización para proporcionar funciones críticas, procesos o servicios por un cierto período de tiempo inaceptable y en el cuál la empresa invoca sus planes de recuperación. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Directorio activo: Término que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos, ofreciendo la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa.

Ejercicio: Proceso para entrenarse, prepararse, practicar y mejorar el desempeño de una organización. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.18]

Emergencia: Un evento o incidente imprevisto que sucede repentinamente y demanda acción e intervención inmediata para minimizar pérdidas potenciales de vidas, destrucción de propiedades o la pérdida o interrupción de las operaciones de negocio hasta el punto que pueda representar una amenaza. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Estrategia de continuidad del negocio: Curso de acción definido previamente (y aprobado por el Comité Directivo - Dirección) con el fin de proteger la viabilidad de la empresa y reanudar sus actividades críticas en los plazos establecidos. Las estrategias seleccionadas deben cubrir los RTOs identificados en el BIA. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Evento: Hecho o suceso imprevisto que puede tener varias causas. Es la ocurrencia o cambio de un conjunto particular de circunstancias. Un evento sin consecuencias puede ser referido como "evento fallido", "incidente", "evento cercano", "evento de aviso" [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.17].

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.51].

Infraestructura: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones, numeral 3.20].

Impacto: Efecto, aceptable o no, que un evento tiene en una organización. Los tipos de impactos al negocio son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos, dependiendo del sector. [Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Incidente: Suceso que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe. [Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Mitigación: Implementación de medidas para disminuir o eliminar la ocurrencia o impacto de un evento. [Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

MTPD (Maximun Tolerable Period of Disruption): Tiempo para que los impactos adversos, los cuales pueden surgir del resultado de no proveer un producto o servicio o realizar una actividad, sea inaceptable. [Norma ISO 22301:2012, Capitulo 3, Términos y definiciones; numeral 3.26]

Plan de Recuperación ante Desastres (Disaster Recovery Plan – DRP): Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Plan de continuidad del negocio (PCN): Conjunto de procedimientos documentados que guían a las entidades para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido aceptable, en caso de interrupciones.

Procesos críticos: Son aquellos procesos que debido a su importancia deben estar disponibles y operativos constantemente o lo antes posible, después de un incidente, emergencia o desastre.

Proveedor: Persona, natural o jurídica responsable de suministrar bienes y servicios. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Respuesta a incidentes: Conjunto de acciones realizadas por una organización ante un desastre u otro evento importante que pueda afectar significativamente a la organización, a su gente o su capacidad de operación normal. Puede incluir: evacuación, activación de un DRP, evaluación de daños o cualquier otra medida necesaria para llevar a la organización a un estatus más estable. [*Disaster Recovery Institute International - DRI International – International Glossary for Resiliency*]

Recovery Time Objective (RTO): Tiempo después de un incidente en el que la operación o el servicio deben ser reanudados.

Recovery Point Objective (RPO): Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.

Riesgo: La posibilidad que tiene una compañía, empresa u organización de sufrir pérdidas de carácter financiero derivadas de la posibilidad de fallos en su propio funcionamiento.

2. Objetivo

Describir las acciones necesarias para la activación del plan de recuperación de desastres DRP en el caso de un evento de riesgo en GeoVictoria, para con ellas asegurar la continuidad de la operación del negocio ante un desastre o contingencia e iniciar de esta manera con el correcto funcionamiento de los servicios identificados como críticos por la empresa y sus clientes.

3. Supuestos

La efectividad de la aplicación del presente documento depende de los siguientes supuestos:

- Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos.
- Los funcionarios que ejecutan este documento, o sus suplentes, se encuentran disponibles y no han sido afectados por el desastre.
- El desastre no afectó simultáneamente el centro de cómputo principal y el centro de cómputo alterno.
- El centro de cómputo alterno estará habilitado para un promedio de 100 usuarios concurrentes.
- Únicamente el funcionario responsable activará el DRP.
- Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han funcionado.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.

4. Alcance

Se presenta la necesidad de desarrollar un plan de recuperación de desastres (DRP) ante el riesgo potencial que provoca la interrupción parcial o total de los servicios de aplicaciones críticas de GeoVictoria, sobre el normal desarrollo de las actividades; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos buscando así mantener el funcionamiento de los sistemas de misión crítica.

Servicios que hacen parte integral del DRP:

Todos los servicios mencionados a continuación se encuentran alojados en Microsoft Azure North Central US localizado en el estado de Illinois.

- App Services: Servicio web que permite a los usuarios la interacción con GeoVictoria y donde pueden generar reportes, consultar y modificar configuraciones y otros servicios. RPO: 1 hora, RTO: 1 hora.
- GvPlanning: Servicio de presentación de reportes. RPO: 1 hora, RTO: 1 hora.
- ReportEngine: Servicio generador de reportes para exportar en varios formatos. RPO: 1 hora, RTO: 1 hora.
- CalculationEngine: Servicio de ejecución de cálculo de datos de los reportes de acuerdo a parámetros. RPO: 1 hora, RTO: 1 hora.
- RawData: Servicio de acceso a fuentes de datos bien sea base de datos, archivos, Azure Storage entre otros. RPO: 1 hora, RTO: 1 hora.
- WriterData: Servicio de actualización de datos bien sea base de datos, archivos, Azure Storage entre otros. RPO: 1 hora, RTO: 1 hora.
- GvAPI: Servicio de API expuesta para integraciones con aplicaciones de terceros. RPO: 1 hora, RTO: 1 hora.
- SQL Server for Azure: Servicio de base de datos hospedado en Azure. RPO: 1 hora, RTO: 1 hora.
- Azure Storage: **Servicio** de Azure para almacenamiento masivo de datos. RPO: 1 hora, RTO: 1 hora.
- Azure Function: Servicios complementarios que permiten la interconexión de sistemas. RPO: 1 hora, RTO: 1 hora.
- BulkUploadEngine: Servicio para cargas masivas de archivos. RPO: 1 hora, RTO: 1 hora.

Los mismos servicios se encuentran alojados en un centro de datos alterno de Microsoft Azure East US localizado en el estado de Virginia.

El cumplimiento del RPO y RTO tanto para el centro de procesamiento de datos cómo para el centro alternativo de datos se verificará en las pruebas realizadas formalmente.

5. Generalidades del plan de recuperación de desastres DRP

De acuerdo con la descripción del alcance GeoVictoria definió unos tiempos de RTO y RPO para cada uno de los servicios, luego de realizar un análisis de criticidad de los mismos, mediante:

RPO (RECOVERY POINT OBJECTIVE): Se define como el periodo máximo en el cual la información de un servicio no estaría disponible con motivo de la ocurrencia de un desastre, puede ser especificado en segundos, minutos, horas o días.

RTO (RECOVERY TIME OBJECTIVE): Corresponde al tiempo que toma y el nivel de servicio mediante el cual un proceso de negocio puede ser restablecido después de la ocurrencia de un desastre o una interrupción del servicio, esto con el fin de mitigar las consecuencias asociadas a la interrupción de un proceso crítico del negocio, en especial, los procesos que deben estar disponibles 24 horas al día todos los días del año.

5.1. Estrategia general de recuperación

Este plan está basado en el hecho de que por alguna situación crítica interna o externa, no haya acceso a los servicios de cómputo centrales por un período inaceptable de tiempo.

Las estrategias para seguir serán acordes a la magnitud y duración tentativa del incidente y se deberán tomar en cuenta los siguientes aspectos:

- Evaluación de los daños.
- Evaluación del tiempo estimado de la recuperación.
- Análisis exhaustivo para determinar las acciones específicas que deberán seguirse de acuerdo con el tipo de incidente.

Este plan solo podrá ser activado únicamente cuando GeoVictoria lo apruebe. Con base en los resultados obtenidos por GeoVictoria en donde se determinó contar con un centro de datos alterno en Microsoft Azure se planteó y estableció la estrategia de recuperación la cual se conforma de elementos tales como tener los servicios alternos disponibles en Microsoft Azure, la preparación y puesta en funcionamiento de un centro de operaciones alterno (COA) y de un centro de monitoreo.

5.2. Estrategia de acción

Las estrategias y planes de acción considerados para la recuperación de GeoVictoria, han sido orientados a cubrir cualquier contingencia mayor o catastrófica que inhabilite el acceso del personal al edificio donde se ubica el centro de operaciones alterno o bien a los servicios de cómputo y telecomunicaciones en que se apoyan las aplicaciones críticas de la entidad, las cuales se definieron como:

1. App Services.
2. GvPlanning.
3. ReportEngine.
4. CalculationEngine.
5. RawData.
6. WriterData.

7. GvAPI.
8. SQL Server for Azure
9. Azure Storage.
10. Azure Function.
11. BulkUploadEngine.

La decisión para desarrollar este plan, se basó en las características de la operación actual de la empresa, así como el nivel de dependencia de tecnología de información y comunicaciones.

Incidencia Menor:
En caso de presentarse una incidencia menor, esta podrá ser subsanada o corregida rápidamente por medio de los mecanismos de detección, diagnóstico y reparación de fallas, activando los procedimientos de atención de problemas utilizados día a día por el personal de GeoVictoria.

Incidencia Mayor:
De presentarse una incidencia mayor en los equipos y sistemas del centro de cómputo principal que impida la función general de la entidad, esta deberá ser identificada y corregida a la brevedad. Si el tiempo estimado de reparación que determinen los equipos de recuperación responsables de las aplicaciones o recursos técnicos críticos, es superior al tiempo identificado para que este operativo, GeoVictoria tomará la decisión de activar o no el plan de recuperación de desastres.

Incidencia Catastrófica:
Si se presenta un incidente que provoque una contingencia catastrófica evidente y que por consiguiente interrumpa las operaciones de GeoVictoria en los Cloud Services de Microsoft Azure. Es importante aclarar que la declaración de contingencia es responsabilidad únicamente de GeoVictoria.

5.3. Clasificación de los escenarios de desastre

En esta sección se incluye una clasificación de los posibles escenarios de desastre que pueden suceder.

5.3.1. Pérdida total o parcial de las instalaciones del centro de datos principal

La pérdida total o parcial de las instalaciones de Microsoft Azure puede deberse a diferentes situaciones y/o motivos tales como:

- Guerras internacionales o civiles.
- Actos perpetuados por terroristas y/o grupos armados ilegales.
- Hostilidades u operaciones bélicas ya sea o no declarada una guerra.
- Rebelión, sedición, usurpación o retención ilegal del mando.
- Asonada, motín, o conmoción popular.
- Huelgas, conflictos colectivos de trabajo o suspensión de hecho de labores y por movimientos subversivos y/o acciones terroristas y/o de grupos armados ilegales que conlleven a daños materiales en las instalaciones.
- Deslizamientos de tierra y/o otros elementos, avalanchas, fallas geológicas, terremoto, temblor, asentamientos, inconsistencias del suelo, inundaciones, erupción volcánica, vientos o cualquier otra convulsión de la naturaleza.
- Reacción o radiaciones nucleares o contaminación radioactiva.

5.3.2. Pérdida total o parcial de los servicios pactados dentro del alcance del plan

La pérdida total o parcial de los servicios pactados dentro del alcance del plan puede originarse por las siguientes causas y/o motivos:

- Daños causados directamente por personas encargadas de la infraestructura de IT, en el curso de la ejecución de las operaciones llevadas a cabo con el propósito de dar cumplimiento a sus obligaciones.
- Por la pérdida de aquellos bienes cuyo valor excede el de los materiales que los componen tales como planos, modelos, metodologías, documentos de cualquier clase, archivos magnéticos y/o cualquier otro medio de archivo computacional, que traiga como consecuencia que no se pueda efectuar la operación normal de los servicios del negocio.
- Por la omisión de los procedimientos establecidos para la prestación de los servicios del negocio.

- Por delitos por computador y/o medios electrónicos que puedan afectar la prestación de los servicios del negocio.
- Por utilización de técnicas como el acceso a los activos de información por medio de una identidad falsa, la alteración de datos en forma no autorizada, la negación de la ocurrencia de un acción o transacción, la visualización de información no autorizada, la negación del servicio y/o operación de el(los) servicio(s) y la obtención del acceso a la plataforma y/o a los aplicativos con todos los privilegios y/o roles que conlleven a la pérdida total o parcial de los servicios del negocio.
- Por las vulnerabilidades en sistemas operativos y/o en las aplicaciones que estén alojadas en el centro de procesamiento de datos.
- Por la disminución en el rendimiento laboral de las personas a cargo de los procesos de negocio.
- Por exposición de accesos lógicos tales como puertas traseras, ataques asíncronos, fuga de datos, intercepción de líneas (wire-trapping), wardriving, dispositivos adosados (piggybacking), cierre de computadores (shutdown), ataques de negación de servicio, redondeo hacia abajo, técnicas de salami, caballos de Troya, virus, gusanos y bombas lógicas que generen la pérdida total o parcial de los servicios de negocio.
- Por exposición de acceso físico tales como entradas no autorizadas, daño, vandalismo o robo de equipos o documentos, copia o visualización de información privada, alteración de equipos e información sensible, revelación al público de información privada, abuso de los recursos de procesamiento de datos que conlleven a la pérdida total o parcial de los servicios de negocio.
- Por problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética, caída de intranet del servicio de Microsoft Azure, caída de backbones que alteren y/o interrumpan el normal funcionamiento de los equipos que se utilicen para los procesos de negocio.
- Por problemas y exposiciones en bases de datos tales como procesamiento interno erróneo, actividad errónea de administración de base de datos, corrupción de la base de datos, acceso indebido a la base de datos para modificarla, errores en puesta en producción/regresión con impacto en base de datos y errores en generación y restauración de respaldos que conlleven a la pérdida total o parcial de los servicios de negocio.
- Por problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques externos para obtención/modificación indebida de información, y la inestabilidad del rendimiento del hardware y/o software que conlleve a la pérdida total o parcial de los servicios del negocio.
- Por acciones tomadas por personas que terminen en el sabotaje de los procesos de negocio a causa de chantaje, fraude, descontentos, huelgas, amenazas (acción disciplinaria o con despido), adictos y/o experimentación de problemas financieros o emocionales.

- Dolo y/o imprudencia manifiesta por parte de personas directa y/o indirectamente involucrada en los procesos de negocios que conlleven a la suspensión total o parcial de los servicios.
- Pérdida del hardware, software y data de propiedad y/o tenida a cargo, en custodia y/o control de GeoVictoria.
- Pérdida o daño debido al cálculo o diseño erróneo del hardware y/o software.
- Falla y/o daño eléctrico interno o desarreglo de los equipos y dispositivos del centro de procesamiento de datos.
- Daños y/o fallas atribuibles a la falta y/o carencia de diligencia en los mantenimientos predictivos, preventivos y correctivos a los equipos y dispositivos del centro de datos.
- Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor, y/o los medios empleados para extinguir y/o contener un incendio ya sea por acción directa e inmediata del mismo, y las demoliciones que sean necesarias a consecuencia del incendio y que sean ordenadas en tal carácter por la autoridad competente.
- Por la combustión espontánea de algún elemento que forme parte de algún equipo y/o dispositivo del centro de procesamiento de datos.

5.3.3. Interrupciones al negocio o incidentes que podrían afectar el cumplimiento de las labores de los funcionarios

Las interrupciones al negocio o incidentes que podrían afectar el cumplimiento de las labores de los funcionarios pueden deberse a diferentes situaciones y/o motivos tales como:

- Pérdidas de personal (Cesación, muerte, accidentes laborales, enfermedades, pandemias).
- Cortes de servicio de transporte en los casos de requerirse.
- Fallas en los proveedores.

5.4. Centro de datos alterno

El sitio alterno para los servicios de GeoVictoria es Microsoft Azure East US localizado en el estado de Virginia en Estados Unidos de América.

La infraestructura del centro de datos provista por Microsoft provee el hardware, software y redundancia de datos requerida para garantizar la continuidad del negocio en caso de presentarse un desastre o una interrupción del servicio, esto incluye redundancia en sitios geográficamente separados, redundancia local entre varios servidores del mismo centro de cómputo, redes de alta velocidad y todo con nivel de servicio del 99.99999999999999% (16 nueves).

Los detalles de la infraestructura de Microsoft Azure pueden ser consultados directamente en la documentación en la página de Microsoft en https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy y un esquema para recuperación de desastres cómo lo detalla el documento de Microsoft https://docs.microsoft.com/en-us/azure/storage/common/storage-disaster-recovery-guidance?toc=/azure/storage/blobs/toc.json.

5.5. Canales de comunicaciones

Microsoft Azure donde se alojan todos los servicios de GeoVictoria cuenta con una infraestructura de comunicaciones robusta que puede ser consultada en detalle en el documento de Microsoft https://docs.microsoft.com/en-us/azure/networking/networking-overview y que ofrece múltiples canales de comunicación con los servicios alojados en los Cloud Services en caso de presentarse un desastre catastrófico acorde a lo descrito en el documento https://docs.microsoft.com/en-us/azure/networking/working-remotely-support.

Todos los servicios de GeoVictoria se encuentran hospedados en Microsoft Azure por lo que un desastre en las instalaciones locales de la empresa en Santiago de Chile o en cualquiera de los otros países donde tiene presencia no afecta la disponibilidad de servicio, y dado que no depende de máquinas locales para la puesta en marcha de los servicios virtualmente desde cualquier computador conectado a Internet puede ingresar a los servicios de Microsoft Azure para ejecutar el plan de recuperación de desastres.

5.5.1. Centro de monitoreo

Microsoft Azure cuenta con mecanismos fiables de monitoreo de los servicios con acceso remoto por personal autorizado de la empresa y alertas de indisponibilidad de servicio en caso de presentarse.

Cómo parte del proceso de monitoreo los servicios de GeoVictoria generan logs para trazabilidad de la operación y se vale de los mecanismos de monitoreo de Microsoft Azure para la vigilancia de los servicios puestos en producción y de sus servicios redundantes.

Detalles sobre los mecanismos de monitoreo ofrecidos por Microsoft se pueden consultar en la documentación de Microsoft disponible en https://docs.microsoft.com/en-us/azure/azure-monitor/overview, y detalles sobre el manejo de *logs* en la aplicación se entregan en el capitulo inicial “Logs” del capítulo 2.

5.6. Procedimientos de notificacion, activacion y retorno

Como parte de las estrategias inmediatas ante una posible crisis, se contemplan las tareas que deben efectuarse lo más rápido posible, después de que se presente el incidente, para reducir posibles impactos. En muchos casos, estos procedimientos contemplan la comunicación inicial con clientes y otros contactos externos, así como también direccionamiento de las estrategias de recuperación de las funciones de negocio más críticas.

A continuación, se listan las actividades a ejecutar cuando se active la contingencia, de acuerdo con la presentación de cualquier tipo de evento adverso:

Tabla 2 - Actividades segun contingencia

Tipo de evento	Características	Ejemplos	Respuesta
Desastre	Evento que inhabilita el centro de procesamiento de datos principal para prestar sus servicios. No permite seguir prestando el servicio a sus clientes.	Terremotos, incendio general, fallo eléctrico, terrorismo o similares en las instalaciones de Microsoft Azure.	DRP
Interrupción	Evento que requiere ser evaluado para ser tratado como desastre o como contingencia. Puede llegar a ser considerado como un desastre o una contingencia, dependiendo del impacto que se determine en el manejo de incidentes.	Incendio, atentado terrorista, huelga interno o externo, tanto en las instalaciones de Microsoft Azure cómo en la sede principal de GeoVictoria.	DRP Planes de contingencia
Contingencia	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de informática. No impide el acceso al CDP. En ausencia de plan de contingencia, requiere evaluación que puede llevarla a categoría de desastre.	Fallo de sistemas o servicio, ausencia de personal clave, error en ejecución de procedimientos que conlleve alteración indeseada de datos.	Planes de contingencia

Las fases de activación en orden son:

1. Detección del incidente.
2. Evaluación del incidente.
3. Activación del plan.

4. Comunicación y seguimiento.

Así mismo se listan algunas actividades anexas a las fases definidas anteriormente:

- Registro de Incidentes.
- Evaluación inicial del alcance del incidente y fallos.
- Validar la criticidad de la falla (Contingencia menor, mayor o catastrófica).
- Comunicar al comité.
- Activar Alertas.
- Activar Desastre.
- Activación del plan de recuperación de desastres.
- Ejecución Procedimientos de contingencia.
- Notificación Contingencia.
- Monitoreo y Seguimiento periodo de contingencia.
- Comunicación continúa interna/externa a involucrados.
- Activación de plan de retorno de contingencia.
- Declaración de fin de contingencia.
- Regreso a modo normal de operación.
- Notificación formal de fin de contingencia.
- Actualización del plan de recuperación de desastres.
- Documentación de lecciones aprendidas.
- Actualización Planes de Prueba.
- Fin de Contingencia.

5.6.1. Procedimiento de notificación

Cuando se presenta una emergencia, hay que tener en cuenta que se debe gestionar la notificación de la misma con el ánimo de iniciar con el proceso de activación del plan de recuperación de desastres (DRP). Esta notificación corresponde a una gestión para la activación del plan la cual se describe a continuación:

1. Detección del evento.
2. Informar el evento.
3. Análisis inicial de la situación.
4. Análisis por parte de los administradores.
5. Notificar al líder de grupo.
6. Notificar al líder DRP.
7. Evaluar activación del DRP.

8. Activar el DRP.

La notificación de la indisponibilidad de los sistemas de información o servicios de TI puede llegar por diferentes fuentes, esto va a depender de la naturaleza del evento, del momento en el cual éste suceda y de la fuente que lo causa. Es importante tener en cuenta que el procedimiento de notificación debe estar ligado a los procedimientos de emergencia definidos y establecidos por GeoVictoria.

El proceso mediante el cual se activa la gestión del plan de recuperación de desastres, previa notificación del desastre, y hasta el momento en que el servicio es restaurado en el centro de procesamiento de datos en producción, se describe de la siguiente manera:

1. Ocurrencia del desastre.
2. Contingencia declarada.
3. Inicio procedimiento de activación del DRP.
4. Operación en centro de cómputo alterno.
5. Finalización de emergencia declarada.
6. Inicio de procedimiento de retorno a centro de cómputo principal.
7. Operación normal en centro de cómputo principal.

El procedimiento de entrada a contingencia describe las actividades requeridas para la activación de los diferentes servicios que se encuentran respaldados en el centro de procesamiento de datos, cuando se activa el plan de recuperación de desastres.

5.6.2. Detección del evento

Los eventos que afectan la continuidad del negocio y servicios identificados como críticos por GeoVictoria, podrán ser reportados luego de ser identificados con el fin de iniciar los trabajos de recuperación y así dar cumplimiento con los RTO's y RPO´s definidos.

Esta detección de eventos se realizará una vez se presenten interrupciones de los servicios que fueron definidos por GeoVictoria cómo críticos:

1. App Services.
2. GvPlanning.
3. ReportEngine.
4. CalculationEngine.
5. RawData.
6. WriterData.
7. GvAPI.
8. SQL Server for Azure
9. Azure Storage.
10. Azure Function.
11. BulkUploadEngine.

5.6.3. Definición de recursos

Como parte del plan de recuperación de desastres (DRP), se realizó la definición de los siguientes recursos, cuyos miembros de los equipos de trabajo atenderán las solicitudes realizadas por GeoVictoria, teniendo en cuenta las responsabilidades específicas que les han sido asignadas.

- Comité de emergencias: Hace parte de la contingencia en la presentación de un evento adverso, este equipo de emergencias debe ser definido internamente en la entidad y en él se debe mantener informado al responsable de la activación de la contingencia.
  Sus principales funciones son:
  - Activación.
  - Declaración.
  - Comunicación.

- Comité responsable de activación: se encuentra conformado por los responsables de la activación del plan de recuperación de desastres DRP.
  Sus principales funciones son:
  - Validación
  - Evaluación.
  - Activación.
  - Coordinación.
  - Integración.
- Equipo de recuperación DRP: Incluye todo el personal técnico de la oficina de informática de la empresa, encargados de realizar la activación de los servicios definidos como críticos y la puesta en funcionamiento de los servicios contemplados dentro del alcance.
  Sus principales funciones son:
  - Ejecución.
  - Verificación.
  - Documentación.
  - Validación.
  - Coordinación.
  - Integración.

5.6.3.1. Comité de emergencias

Realiza la evaluación de los daños y la magnitud del suceso, trabaja de la mano con el equipo de DRP, y su principal función es salvaguardar las vidas humanas, este comité es informado lo antes posible de cualquier evento disruptivo para la toma de decisiones efectivas para la superación de eventos y dar alcance a la comunicación oportuna al líder de DRP para iniciar a la activación de los servicios definidos en el alcance. La intervención de este grupo durante una situación de contingencia está determinada por el tipo de daño, siendo necesaria su gestión en la ocurrencia de algún evento.

Hace parte del comité de emergencias el equipo evaluador de daños quienes validan los daños a la infraestructura de IT y sus servicios con el fin de determinar la afectación y poder informar con el comité de emergencias al comité de activación DRP si se debe declarar una contingencia. La intervención de este grupo durante una situación de contingencia está determinada por el tipo de daño, siendo necesaria su gestión en la ocurrencia de algún evento.

Participante:

- Equipo evaluador de daños.

Funciones específicas:

- Evaluar los daños físicos que se presenten en la infraestructura de IT y sus servicios asociados, cuando haya ocurrencia de un desastre.
- Presentar al comité de emergencias el status de afectación de la infraestructura.
- Participar en la toma de decisión para declarar un desastre y activación del DRP.
- Realizar un análisis de los servicios en funcionamiento con el fin de determinar si los funcionarios responsables de las aplicaciones críticas deben activar la redundancia de servicios en el COA.

5.6.3.2. Comité de responsable de activación del DRP

Está conformado por el jefe de la oficina de informática. Esto no es una limitante en caso que se decida invitar a participar dentro de este equipo a algunos funcionarios del nivel ejecutivo de GeoVictoria como el mismo director general, subdirectores o jefes de área. No se debe perder de vista el carácter técnico del DRP y por tanto el nivel de especialización del equipo.

Se debe asegurar la comunicación permanente con las altas directivas de GeoVictoria en cada momento (antes, durante y después) por la naturaleza de las decisiones que se deban tomar. El coordinador del DRP y el líder DRP también integran este equipo a nivel de apoyo para la toma de decisiones.

Algunas de las responsabilidades de este equipo son:

- Establecer las directrices y políticas del DRP enmarcadas en un plan de continuidad del negocio, y alineadas con el sistema de gestión de continuidad de negocio.
- Mantener contacto con la alta dirección, proveedores y entidades interesadas, sobre la situación de GeoVictoria.
- Toma de decisiones estratégicas durante la crisis o incidente.
- Declarar la activación del DRP.
- Comunicación efectiva con los medios de comunicación, en caso de no existir un equipo a nivel institucional.
- Supervisión de la efectividad de las actividades de recuperación.

Participante:

- Comité responsable de activación del DRP.

Funciones específicas:

- Mantener comunicado al enlace ejecutivo del desarrollo del plan de contingencia.

- Determinar conjuntamente con el coordinador DRP el plan de respuesta inmediato y el plan de acción de los equipos DRP.
- Monitorear la ejecución del DRP hasta el regreso a modo normal de operación.
- Gestionar la disponibilidad de los recursos técnicos mínimos para la activación de los servicios del DRP.

En conjunto como parte del equipo de trabajo se encuentran:

- Líder DRP.
- Coordinador DRP.

Estas personas tienen a su cargo las siguientes funciones:

Participante:

- Líder DRP.
- Coordinador DRP.

Funciones específicas:

- Garantizar la operatividad del plan de recuperación de desastres.
- Planear y coordinar las pruebas del plan de contingencias en conjunto con el líder DRP.
- Identificar los responsables para la administración, mantenimiento y ejecución de pruebas de la contingencia en conjunto con el líder DRP.
- Ejecutar las actividades de divulgación y capacitación del plan de contingencias.
- Evaluar el incidente reportado y estimar el impacto en la operación de los servicios.
- Proporcionar toda la información necesaria al comité directivo de contingencias para que se declare la situación de contingencia.
- Notificar y alertar a los equipos de recuperación correspondientes. Registrar los eventos y acciones desarrolladas durante el estado de contingencia.
- Coordinar todas las actividades que se requieran realizar en el centro de procesamiento de datos alterno de común acuerdo con el personal técnico de la empresa y con el centro de procesamiento de datos principal en caso de que sean equipos distintos.
- Brindar servicios de calidad en los tiempos esperados (RPO y RTO) y garantizar la continuidad del servicio.
- Definir, implementar y documentar nuevos procedimientos y acciones de mejora.
- Consolidar los informes de gestión, estadísticas y demás información de los servicios implementados que le competan.

- Supervisar todo cambio realizado en las instalaciones de la infraestructura tecnológica (cómo cambios en la infraestructura configurable de Microsoft Azure) y en sus servicios asociados.

5.6.3.3. Equipo de recuperación DRP

Está compuesto por:

- Equipo evaluador de daños.
- Coordinador DRP.
- Especialistas.
- Equipo de soporte a usuarios (Jefes de Proyectos).

Recibe la confirmación de activación del DRP del comité responsable de activación del DRP y se encarga de restablecer la operación de los servicios de software, telecomunicaciones y seguridad física que dificulten la continuidad de la operación en el sitio principal.

Participante:

- Equipo recuperación DRP.

Funciones específicas:

- Llevar a cabo los procedimientos de recuperación de la operación cuando de declare la contingencia, en coordinación con los responsables designados de cada proceso.
- Ejecutar el plan de pruebas para los pasos a seguir en el retorno a producción.
- Mantener un inventario y registro actualizado de los servicios y componentes que integran la infraestructura tecnológica a recuperar.
- Mantener actualizados las copias de respaldo y documentos necesarios para la recuperación en caso de eventos o contingencias.
- Identificar y documentar los requerimientos mínimos para la operación de las aplicaciones.
- Identificar las debilidades de la infraestructura en Microsoft Azure frente al escenario de contingencia.
- Mantener actualizados los listados de contactos técnicos, proveedores y equipos de contingencia con datos de ubicación (teléfono, celular, dirección, e-mail) para emergencias.
- Evaluar el tipo de daño ocurrido sobre los servicios reportados.
- Informar al equipo coordinador de contingencias sobre el evento.
- Ejecutar los procedimientos de activación del plan de contingencia establecidos previamente.
- Contactar a los proveedores o personas responsables para superar la contingencia.
- Informar al equipo coordinador de contingencias sobre el avance y el tiempo de recuperación estimados.
- Ejecutar las acciones de recuperación pertinentes a cada acción desarrollada.
- Evaluar la efectividad del plan de contingencias para su área de responsabilidad.
- Actualizar los procedimientos existentes.

- Modificar las tareas y procedimientos del equipo de trabajo según sea necesario.
- Realizar informe de las actividades desarrolladas, resultados y lecciones.

Dentro del equipo de recuperación DRP se encuentran los diferentes roles de especialistas en cada una de las áreas junto con sus responsabilidades de la siguiente manera:

5.6.3.4. Equipo de la plataforma Azure

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios específicos de la plataforma Azure sobre los cuales funcionan los servicios identificadas como críticos y los servicios que los apoyan, desde el centro de procesamiento de datos alterno.

Igualmente es responsable de todas las actividades que garanticen la adecuada disponibilidad del servicio de respaldo en cuanto la actualización de los sistemas, aplicativos, datos y documentación, y las que conduzcan al restablecimiento de los servicios desde el centro de procesamiento de datos principal.

Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y arranque de los servicios y los planes recuperación.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de desastre.
- Mantener iguales las configuraciones de Microsoft Azure y de los servicios del centro de procesamiento de datos principal y del centro de procesamiento de datos alterno.
- Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- Definir y ejecutar pruebas del DRP en lo referente a esta plataforma.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el centro de procesamiento de datos alterno.
- Asistir la recuperación de la plataforma en el centro de procesamiento de datos principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el centro de procesamiento de datos principal.
- Alistar el centro de procesamiento de datos alterno para usarlo nuevamente después de un retorno a la normalidad.

5.6.3.5. Equipo de base de datos y almacenamiento

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios específicos sobre los cuales funcionan las bases de datos y almacenes de datos de los servicios

identificados como críticos y los servicios que los apoyan, desde un centro de procesamiento de datos alterno.

Igualmente es responsable de todas las actividades que garanticen la adecuada disponibilidad del servicio de respaldo en cuanto la actualización de datos y documentación, y las que conduzcan al restablecimiento de los servicios desde el centro de procesamiento de datos alterno.

Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y arranque de los servicios de base de datos y los planes recuperación.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Verificar la realización de las copias de seguridad.
- Verificar el estado de la actualización, se debe procurar que los datos del centro de datos principal y el del centro de datos alterno, esté al mismo nivel de actualización.
- Tener disponibilidad de los medios de instalación de los gestores de bases de datos.
- Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- Definir y ejecutar pruebas del DRP en lo referente a esta plataforma periódicamente o cuando se tenga contemplado con el proveedor.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el centro de procesamiento de datos alterno.
- Asistir la recuperación de la plataforma en el centro de procesamiento de datos principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el centro de procesamiento de datos principal.
- Alistar el centro de procesamiento de datos alterno para usarlo nuevamente después de un retorno a la normalidad.

5.6.3.6. Equipo de Conectividad

Es el responsable de planear y coordinar las actividades que permitan la activación de los servicios específicos de conectividad sobre los cuales se apoya la entrega de los servicios de telecomunicaciones en un centro de procesamiento de datos alterno, específicamente la activación de conectividad desde los servicios replicados en Microsoft Azure.

Igualmente es responsable de todas las actividades que garanticen la adecuada disponibilidad del servicio de respaldo en cuanto la actualización de los sistemas, aplicativos, datos y documentación, y las que conduzcan al restablecimiento de los servicios desde el centro de procesamiento de datos principal.

Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y configuración de conectividad en Microsoft Azure.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Mantener iguales las configuraciones de los equipos del centro de procesamiento de datos alterno y centro de procesamiento de datos principal.
- Definir y ejecutar pruebas del DRP cuando se tenga establecido con el proveedor.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el centro de procesamiento de datos alterno.
- Asistir la recuperación de la plataforma en el centro de procesamiento de datos principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el centro de procesamiento de datos principal.
- Alistar el centro de procesamiento de datos alterno para usarlo nuevamente después de un retorno a la normalidad.

5.6.3.7. Equipo de administradores de la aplicación

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios en los respectivos servidores de tal forma que se restablezcan los servicios del negocio en un centro de procesamiento de datos alterno.

Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y arranque de los servicios.
- Mantener actualizado los requerimientos para la operación de los servicios.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Velar porque las configuraciones de los servicios en el centro de procesamiento de datos alterno y en el centro de procesamiento de datos principal sean apropiadas para el correcto funcionamiento de los servicios.
- Velar porque las versiones de las aplicaciones disponibles en el centro de procesamiento de datos alterno y el centro de procesamiento de datos principal sean las mismas.
- Definir y ejecutar pruebas del DRP en lo referente a las aplicaciones.
- Definir y apoyar la ejecución de las pruebas del DRP.
- Velar porque se realicen los respaldos a la aplicación de acuerdo con las necesidades.
- Mantener los contratos de soporte de acuerdo a lo requerido por GeoVictoria.

- Atender los requerimientos de auditoria.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el centro de procesamiento de datos alterno.
- Proveer soporte técnico según requerimientos del momento.
- Documentar fallas y su solución.
- Asistir la recuperación de las aplicaciones en el centro de procesamiento de datos principal.
- Restaurar el servicio en el centro de procesamiento de datos principal.
- Alistar el centro de procesamiento de datos alterno para usarlo nuevamente después de un retorno a la normalidad.

5.6.3.8. Equipo de soporte a usuarios (Jefes de Proyectos)

Corresponde al grupo de personas que han sido identificadas como responsables funcionales de los aplicativos que utilizan los servicios prestados por la oficina de informática para ejecutar las funciones propias de su proceso y otras complementarias al trabajo diario.

Algunas de las responsabilidades de los usuarios son:

- Información y notificación de eventos identificados a nivel de sus procesos que puedan afectar las operaciones.
- Participar en las actividades de continuidad (capacitaciones, divulgación, pruebas y auditorias).
- Actualizar la información de continuidad de las operaciones internas de su proceso y divulgarlos al interior del mismo. En este proceso se deberá seguir los lineamientos de control documental y de versiones de GeoVictoria.
- Participar en los ajustes a las actividades de entrevista de valoración de impacto de negocio y evaluación de riesgos a nivel de proceso.
- Apoyar al interior de su proceso los aspectos de continuidad, indicando acciones de mejora, cambios al interior del proceso y otros factores que deban ser revisados a nivel de comité para su aprobación.

El equipo de soporte a usuarios debe brindar el soporte a los usuarios finales de la empresa para el desarrollo de sus actividades durante el tiempo que esté operativa la contingencia.

El equipo está conformado por:

- Coordinador de Jefes de Proyectos.
- Jefes de Proyectos.
- Operadores de centro de procesamiento de datos alterno.

Responsabilidades:

- Conocer y entender el plan de contingencia.
- Verificar con los usuarios finales de GeoVictoria la estabilidad de las aplicaciones y reportar anomalías.
- Cooperar con el equipo de recuperación de contingencias en la puesta en marcha del plan de contingencia.
- Actualizar los procedimientos existentes en el manual de contingencias que esté relacionado con su trabajo.

5.6.4. Árbol de llamadas

El árbol de llamadas representa la cadena de llamadas que se debe seguir y cumplir para comunicar a los integrantes del DRP la activación del plan, esta se ejecuta después de la declaración de contingencia realizada por el líder DRP.

El árbol de llamadas está dividido en equipos o grupos para permitir llamar a los integrantes requeridos según el tipo de contingencia que se haya declarado.

Cada nivel está encargado de llamar al nivel inferior según la estructura del plan y el llamado a cada integrante debe ser verificado por el nivel superior. El jefe de la oficina de informática y su líder DRP son los encargados de efectuar las llamadas y son los responsables de la comunicación con el primer nivel de llamadas.

El llamado a los integrantes del plan se debe realizar siguiendo el procedimiento de comunicación necesario y utilizando los medios de comunicación disponibles para realizarlo.
A continuación, se relacionan algunos medios de comunicación a ser utilizados al momento de un evento adverso, así como su prioridad en usabilidad:

Tabla 3 - Medios de Comunicacion

Medios de comunicación		
Prioridad	Tipos de medio	Descripción
1	Persona a persona	La forma directa y efectiva de comunicar el evento es hacerlo persona a persona. Esté medio permite ser más explícito y detallar lo sucedido con el evento. La comunicación depende de factores socio-ambientales y/o factores de riesgo (catástrofes) que afecten este tipo de comunicación.
2	Telefonía celular	La comunicación telefónica es un medio facilitador para acortar distancias y tener una conversación interpersonal. Con
3	Telefonía fija	

4	Microsoft Teams (requiere smartphone ó computador, además de Internet)	él se puede al igual que en la comunicación persona a persona ser más explícito y profundizar dentro de la comunicación del evento.
5	Radios de dos vías (walkie talkie)	Es un medio de comunicación predilecto en áreas de seguridad y para las brigadas de emergencias. Tiene restricciones de distancia y de uso.
7	Mensajería instantánea y/o Zoho (requiere computador ó smartphone, además de internet. WhatsApp (requiere smartphone e internet)	La mensajería instantánea como un tipo de correo permite interactuar más rápida y efectivamente entre una o varias personas. Depende de los medios y restricciones impuestos por la empresa y de la disposición de los intercomunicadores.
8	Correo electrónico	El correo electrónico se ha establecido como un medio efectivo para comunicarse a cualquier distancia y en el menor tiempo. Este tipo de comunicación depende del grado de consulta de los intercomunicadores.
9	Correo físico certificado	El correo certificado permite enviar documentos de forma más segura a cualquier destinatario. Este tipo de medio permite realizar un seguimiento vía Internet a los paquetes y/o documentos enviados.
10	Correo físico normal	El correo físico normal, es uno de los medios más antiguos y que sigue teniendo vigencia. Este depende de los medios de transporte y las distancias para asegurar una buena efectividad.
11	Redes sociales (Facebook, Twitter, Instagram)	Para ubicar a las personas de los diferentes equipos del DRP.

5.7. Pruebas del plan de recuperación de desastres DRP

Realizar pruebas es parte del ciclo de vida plan de recuperación de desastres, dichas pruebas se realizan con el fin de encontrar discrepancias, faltantes o desactualizaciones del plan de recuperación establecido.

Todas las personas involucradas y descritas en la sección anterior deberán participar en la actualización del DRP y en la realización de las pruebas de todo el plan mejorando así la calidad y efectividad del mismo para afrontar un evento disruptivo que atente contra la operación del negocio.

5.7.1. Divulgación del DRP

Uno de los mayores riesgos de un DRP es la falta de divulgación del plan a todo el personal involucrado ya que ocurrido un evento disruptivo el plan de recuperación de desastres puede ser mal aplicado generando así un evento catastrófico para la empresa y/o sus clientes.

Se deben realizar periódicamente capacitaciones y actualizaciones a todo el personal de la empresa del DRP actual y de sus cambios, así mismo se deben hacer partícipes de los simulacros que se realicen. Las capacitaciones para informar del DRP al personal de GeoVictoria deben tener la máxima prioridad sobre otros procesos de la empresa ya que omitir la divulgación del DRP puede desencadenar en pérdidas económicas y reputacionales para GeoVictoria que en algunos casos pueden ser irrecuperables.

5.7.2. Verificación de respaldos de datos

El equipo de base de datos y almacenamiento debe verificar los almacenes de datos (Azure Storage) y bases de datos contra los últimos desarrollos publicados para verificar que los respaldos de los datos sean adecuados y estén actualizados de modo que corresponda con la última versión de los servicios en ejecución en el centro de procesamiento de datos principal y alterno.

Se deben verificar además los procedimientos de generación y restauración de respaldos en disco y de su almacenamiento en sitios alternativos para poderlos recuperar en caso de un evento disruptivo y cumplir así con los tiempos RTO’s y RPO’s.

En caso de encontrarse inconsistencias con los procedimientos actuales se debe actualizar la documentación de acuerdo a los hallazgos encontrados y se ejecutarán las pruebas de generación de respaldos, almacenamiento de los mismos y de su restauración para verificar su efectividad en caso de un desastre potencial.

5.7.3. Verificación de procedimientos y roles

Junto con todo el personal involucrado en el DRP se deben verificar los roles de cada persona y sus funciones, así cómo la reasignación de funciones en caso de cambios en el personal por retiros, enfermedad, cambios de cargo o muerte. Igualmente se debe verificar las funciones con el objetivo de recordarle a cada actor involucrado en el DRP su importancia y las situaciones individuales que deberá afronta en caso de un evento disruptivo.

Por otra parte, se deben verificar todos los procedimientos de monitoreo de los servicios, la activación del DRP, la generación y restauración de respaldos de la información y de las versiones de software de producción, la verificación del centro de procesamiento de datos alterno. En caso de requerirse cambios por procesos obsoletos, por falta de pasos o por cambios en el entorno de la organización entonces se deberán convocar reuniones para actualizar el DRP y ejecutar nuevas pruebas de verificación del mismo luego de los cambios propuestos para generar las correcciones que apliquen.

5.7.4. Análisis de probabilidades de eventos disruptivos

Las condiciones que generan riesgos para la operación del negocia cambian constantemente por cambios políticos, climáticos, de salud, sociales y económicos que obligan al DRP a ser actualizado a las nuevas condiciones de su entorno y también a los cambios tecnológicos naturales dentro de la empresa que constantemente adopta nuevas y mejores tecnologías de la información.

Se debe realizar un análisis del cambio de probabilidades de los eventos disruptivos a medida que las condiciones del entorno van cambiando para actualizar las prioridades y estar preparados para los principales eventos de posible ocurrencia, de encontrarse falencias en el DRP actual debe ser actualizado de inmediato y probado en su totalidad para verificar su efectividad.

En el análisis de probabilidades de eventos disruptivos deberán participar todos los equipos detallados en la sección anterior con el fin de que cada equipo realice el análisis de acuerdo a sus funciones específicas asignadas.

5.7.5. Preparación de escenarios posibles

Para la correcta ejecución de las pruebas del DRP se deben considerar todos los escenarios posibles de eventos disruptivos organizados por prioridad y probabilidad de ocurrencia ocupándose primero por los más importantes y probables y por su efecto negativo en caso de ocurrencia para la empresa y sus clientes.

Dentro de los escenarios posibles se deben considerar:

- Pérdidas de personal (Cesación, muerte, accidentes laborales, enfermedades, pandemias).
- Cortes de servicio de transporte.
- Fallas en los proveedores.
- Cambios sociopolíticos y económicos.
- Cambios tecnológicos y obsolescencia.
- Desastres naturales.
- Problemas de salud pública cómo pandemias y enfermedades generales.
- Cambios climáticos.
- Guerras.
- Pérdida de respaldos de información.
- Pérdidas de conectividad con los Cloud Services.
- Entre otros factores.

Para cada escenario posible se debe plantear una estrategia para abordarlo y simularlo sin afectar los servicios en el centro de procesamiento de datos principal y poder estar en la capacidad de reversar y repetir las pruebas sin consecuencias para la operación de GeoVictoria ni para sus clientes.

5.7.6. Frecuencia de las pruebas DRP

Todas las pruebas mencionadas se verifican y ejecutan cada seis meses con todos los equipos involucrados en el DRP y tan pronto finalizan las pruebas se acuerdan comités de revisión de resultados para realizar los ajustes que se requieran y planear nuevas pruebas.

En caso de presentarse alguna duda sobre la efectividad del DRP actual no es necesario esperar los seis meses a la siguiente revisión, cualquier miembro del personal puede proponer revisiones en cualquier momento justificando las mismas basadas en cambios en el entorno de la organización o en sospecha de cambios en las probabilidades de eventos disruptivos.

Luego de la ejecución de cada prueba se deben documentar los resultados así no se consideren cambios en el DRP actual y generar actas de las pruebas realizadas, igualmente realizar la divulgación del DRP con alta prioridad a todo el personal de GeoVictoria en todos los países donde tiene presencia.

PLAN DE CONTINUIDAD DEL NEGOCIO - PCN

Cada vez más las empresas se ven afectadas por los probables eventos disruptivos que pueden afectar la continuidad de su negocio y en algunos casos pueden llevar a la empresa a una crisis irrecuperable, es por ello que se implementan planes, procedimientos, y estructuras que garanticen la continuidad de sus productos y servicios críticos ante posibles eventualidades.

Los eventos de riesgo cada vez son más dinámicos y así mismo los planes de la empresa para afrontar los posibles riesgos también deben ser dinámicos y adaptarse continuamente a los cambios en el entorno de la empresa, enfrentado ahora temas que antes no se consideraban parte del plan cómo terrorismo, paros nacionales, la globalización, las ciber-amenazas, pandemias y otros factores.

1. Objetivo

Establecer premisas y lineamientos a seguir en un evento disruptivo para permitir la continuidad de los servicios críticos de GeoVictoria.

2. Definiciones

Análisis de impacto en el negocio: Dentro de la gestión de la continuidad del negocio, es la tarea que identifica las funciones vitales del negocio y sus dependencias. Estas dependencias pueden incluir proveedores, personas, procesos de negocio, servicios y otros.

Equipo funcional: Personal que integra el proceso.

Evento disruptivo: Un evento que impacta la capacidad de una organización para continuar sus operaciones.

Plan de contingencia: Es un plan de respuesta a una emergencia, incluidas las operaciones de *backup* y recuperación post-desastre gestionadas por la organización como parte de su programa de seguridad, garantizando de éste modo la disponibilidad de recursos críticos y facilitando la continuidad de las operaciones críticas en una situación de emergencia.

Plan de continuidad del negocio (PCN): Conjunto de procedimientos documentados que guían a las entidades para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido aceptable, en caso de interrupciones.

Políticas: Son criterios generales de ejecución que complementan el logro de los objetivos y facilitan la implementación de las estrategias.

Proveedor: Entidad encargada de abastecer un servicio o producto necesario para que desarrolle su actividad principal.

3. Desarrollo

3.1. Generalidades

El plan de continuidad del negocio reúne un conjunto de procedimientos que mantienen el normal funcionamiento de la empresa y la prestación de sus servicios críticos, este plan establece los procedimientos en los siguientes tres momentos:

- Preventivo: Dentro de este aspecto se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan prever a la gestión en los diferentes procesos.
- Reactivo: Este aspecto va dirigido a fortalecer las políticas internas y comunicarlas oportunamente para ponerlas en marcha una vez se detecte una contingencia.
- Recuperación: Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia.

Según el *Business Continuity Institute* – BCI, la continuidad del negocio es una colección de procedimientos e información que es desarrollada, compilada y mantenida en preparación para el uso en el evento de una emergencia o desastre, y el *Disaster Recovery Institute Internacional* define la planeación de la continuidad del negocio cómo el proceso de desarrollar arreglos previos y procedimientos que capaciten a la organización para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción o cambios esenciales.

El plan de continuidad del negocio se enfoca en sostener las funciones de negocio de una organización, durante y después de una interrupción mientras se recuperan en paralelo.

En la siguiente figura se muestra el ciclo de vida del PCN, que inicia en el entendimiento de la organización, luego se determinan estrategias, se procede al desarrollo e implementación, y se prueban los planes generados, por último, se hace mantenimiento y auditorías tanto internas como externas, este ciclo nunca termina y se debe integrar en la cultura organizacional.

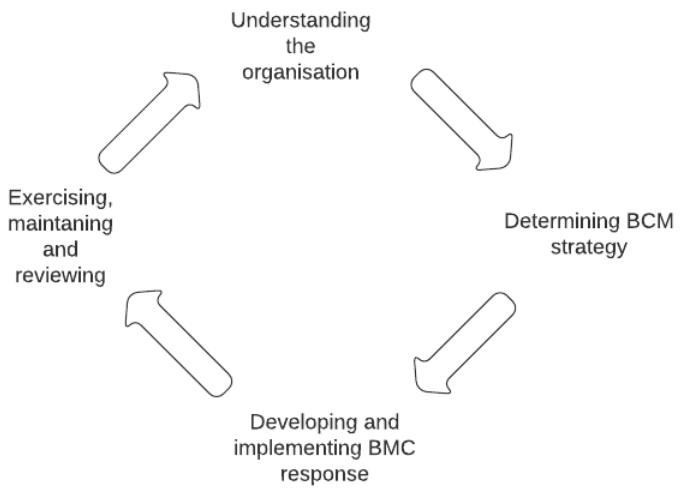


Figura 36 - Ciclo de vida del prgrama PCN

3.2. Plan de continuidad del negocio

Este plan busca sostener en niveles previamente definidos y aceptados, los procesos críticos del negocio a través de la estructuración de procedimientos e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre. Por otra parte, el DRP y los planes de contingencia, forman parte del PCN.

Por otra parte, el Plan de Continuidad del Negocio busca respaldar integralmente los intereses de la organización, así como preservar los indicadores de generación de valor (reputación, marca, confianza con los clientes, entre otros). Asimismo, se busca optimizar la capacidad de recuperar los servicios críticos ante pérdidas importantes en recursos productivos u operativos (personal).

El Plan de Continuidad del Negocio considera 4 fases que son:

- Fase 1: Definición de roles, funciones y competencias.
- Fase 2: Definición de política del plan de continuidad del negocio, esquema documental, procedimiento del plan de continuidad del negocio y esquema de medición.
- Fase 3: Análisis de impacto al negocio – BIA, análisis de riesgos y diseño de estrategias.
- Fase 4: Planes PCN por cada proceso, diseño del plan de pruebas de escritorio y documento preauditoria al plan de continuidad del negocio.

3.2.1. Planes complementarios al plan de continuidad del negocio

El plan de continuidad del negocio se complementa con otros planes que lo apoyan en la respuesta general de continuidad según sea el tipo de evento o el escenario que se presente.

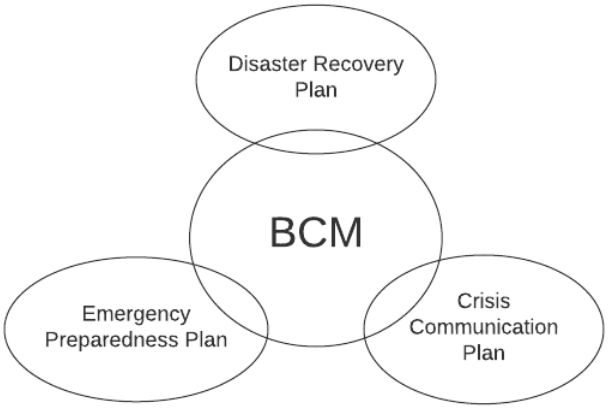


Figura 37 - Relación entre planes de continuidad.

Los planes a saber son:

Plan de comunicación de crisis:
Contiene los procedimientos internos y externos, que garantizan la comunicación efectiva entre los equipos preparados para afrontar la crisis presentada y garantizar que únicamente sea divulgada información autorizada al personal del Plan de Recuperación de Desastres, del Plan de Emergencia y al público en general.

Planes de emergencia:
Contiene los procedimientos que debe seguir el personal de una instalación en el evento que una situación se convierta en una amenaza potencial a la salud y seguridad del mismo, también al medio ambiente o posiblemente a la propiedad, situaciones cómo desastres naturales, ataques vandálicos, emergencias médicas u otros.

Plan de recuperación de desastres - DRP:
Orientado a responder a eventos importantes, su definición y detalles se pueden consultar en el capítulo anterior donde se detalla el DRP de GeoVictoria.

3.3. Metodología

La metodología utilizada para el desarrollo del Plan de Continuidad del Negocio para GeoVictoria propone un proceso que va desde el inicio del proyecto hasta el mantenimiento del plan mismo, lo anterior apoyado en las prácticas proveniente de institutos tales como el Business Continuity Institute, el *Disaster Recovery Institute International*, *National Institute of Standards and Technology*, *International Organization for Standardization* – ISO 27001, *National Fire Protection Association* - NFPA 1600, entre otros.

La metodología comprende las siguientes fases:

1. Inicio del proyecto.
2. Entendimiento de la organización.
3. Análisis de impacto al negocio (*Business Impact Analysis* - BIA).
4. Evaluación de riesgos.
5. Estrategias de continuidad.
6. Comité de crisis.
7. Comunicaciones.
8. Entrenamiento.
9. Pruebas.

3.3.1. Inicio del proyecto

En esta etapa se estructura el plan de continuidad del negocio de modo que se encuentre organizado y controlado para su ejecución con el fin de cumplir sus objetivos. Es importante en esta fase contar con el apoyo de la gerencia de la empresa, formar los equipos de trabajo, los planes complementarios, contar con la participación de expertos en los distintos procesos del negocio y las distintas áreas que componen la empresa para detallar el alcance del proyecto de desarrollo e implementación del plan de continuidad del negocio.

Para GeoVictoria se definió la siguiente política de continuidad del negocio.

Política de continuidad del negocio:
GeoVictoria hace todo lo que esté a su alcance para que, en un tiempo adecuado, ante eventos disruptivos que afecten sus operaciones, los clientes y partes interesadas continúen recibiendo los servicios que GeoVictoria determina como servicios críticos. GeoVictoria establece como premisa ante un evento disruptivo o catástrofe la preservación de la vida e integridad de su personal, contratistas y demás partes interesadas, y el restablecimiento de los servicios de manera priorizada de acuerdo con la

criticidad para el negocio y los niveles de servicio comprometidos con los clientes tanto internos como externos.

Lineamientos generales:

a. El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.

b. Todo el personal de la empresa debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Continuidad del Negocio, además de capacitación del personal nuevo que ingresa a formar parte del equipo de GeoVictoria.

c. En caso de presentarse un incidente significativo se deben aplicar los mecanismos, tanto internos como externos, de comunicación apropiados.

d. Las etapas del plan de continuidad deben ser ejecutadas por cada una de las dependencias de la empresa, con la guía y coordinación del departamento de sistemas e informática.

e. Los jefes de cada dependencia deben designar un Líder de Plan de Continuidad del Negocio, quien es responsable de apoyar las actividades del Programa de Plan de Continuidad de Negocios para la dependencia que representa.

f. Las diferentes etapas que conforman la fase de prevención deben ser ejecutadas con la siguiente frecuencia:
   - El análisis de impacto del negocio debe actualizarse por lo menos una vez al año o cada vez que un Líder de Proceso lo requiera, teniendo en cuenta los cambios de la entidad y sus necesidades.
   - El monitoreo a los riesgos de continuidad se efectuará de acuerdo a la Guía de Administración de riesgos.
   - Se debe realizar por lo menos una prueba anual a las estrategias de contingencia definidas.

g. Los procesos críticos deben ser recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad del Negocio.

h. Los procesos o servicios de la entidad que sean desarrollados por terceros contratados deben disponer de planes de continuidad, para lo cual el funcionario interventor del contrato debe solicitar este documento y remitirlo a la Oficina de Sistemas e Informática, donde se analizará la cobertura del mismo. Adicionalmente, se debe verificar que los planes, en lo que corresponden a los servicios convenidos, funcionen en las condiciones esperadas, donde la Oficina de Sistemas e Informática debe coordinar con la dependencia responsable del contrato la ejecución de pruebas a dicho plan.

i. Los planes de contingencia deben mantenerse actualizados, para lo cual se deben desarrollar, probar y de ser necesario mejorar de forma periódica o ante cambios significativos en políticas, personas, proceso, tecnología; siendo necesario que en dicha revisión participen los líderes de los procesos involucrados.

3.3.2. Entendimiento de la organización

Durante esta fase se recopila la información de los procesos documentados de GeoVictoria y se revisan sus entradas, salidas y activos que requiere el proceso para lograr sus objetivos. También se realizarán entrevistas con cada uno de los dueños de los procesos seleccionados como críticos con el fin de lograr un mejor entendimiento de la organización y así tener las entradas suficientes para proceder a realizar el Análisis de Impacto al Negocio. Esta fase se concentra principalmente en entender la misión, visión, prioridades del negocio, realizar el Análisis de Impacto al Negocio o BIA, y realizar análisis de riesgos.

GeoVictoria define los siguientes procesos en su estructura organizativa.

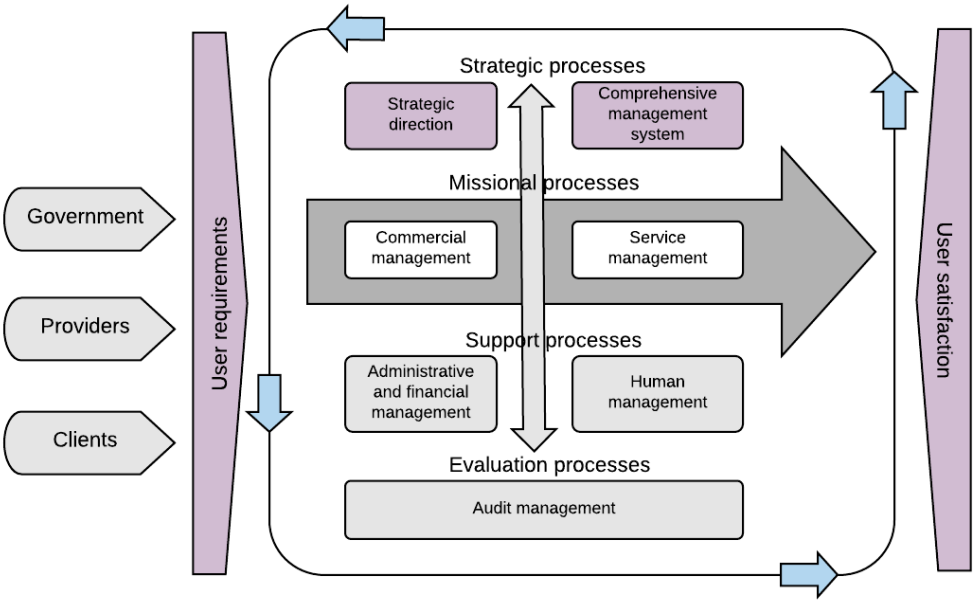


Figura 38 - Modelo de procesos.

3.3.3. Analisis de impacto al negocio

El propósito del Análisis de Impacto al Negocio, conocido comúnmente como BIA, es determinar los productos y procesos críticos que garantizan la continuidad de las operaciones de GeoVictoria y los posibles impactos que se tendrían si éstos no se encuentran disponibles y en correcto funcionamiento. Por otra parte, el BIA permite estimar los tiempos objetivos de recuperación de los procesos críticos con el fin de regresarlos a su operación normal después que ha ocurrido un evento disruptivo y los tiempos de almacenamiento requeridos para disminuir la pérdida de datos.

El análisis de impacto del negocio implica determinar las labores y los recursos esenciales para respaldar la continuidad de las operaciones de GeoVictoria, su criticidad, su impacto para el negocio, sus RTO's y RPO's. También es parte del análisis de impacto del negocio el entendimiento y comportamiento de sus diferentes productos y servicios críticos.

Para el desarrollo del análisis de impacto del negocio, como se mencionó anteriormente, es muy importante, además de entender los productos y servicios críticos de la organización.

Los procesos considerados fueron:

a. Procesos Misionales
   - Docencia
   - Investigación
   - Capacitación
   - Asesoría y asistencia técnica
b. Procesos de Apoyo
   - Gestión tecnológica
   - Gestión financiera
   - Gestión del recurso humano

A continuación, se presentan las actividades, entradas y productos relacionados con la metodología del análisis de impacto del negocio:

1. Planeación del análisis de impacto del negocio.
2. Levantamiento de la información.
3. Análisis de la información.
4. Informe de resultados.

En esta fase se planea la estructura conceptual para el desarrollo de las fases posteriores y se diseñan también los formatos de los documentos requeridos en cada una de estas fases:

1. Entender previamente los procesos del negocio de GeoVictoria sobre los que se realizará el análisis de impacto del negocio.
2. Definir qué aspectos del negocio se desean cubrir con la información que se suministrará.
3. Identificar el personal a ser entrevistado.
4. Definir los cuestionarios a utilizar para recolectar la información, capacitar a los entrevistadores, unificar criterios y términos utilizados.
5. Definir las fechas en que se realizarán las entrevistas.

Levantamiento de información:

En esta fase se realizan las entrevistas con el objetivo de recolectar la información requerida para ser analizada en la siguiente fase (Análisis de la Información).

1. Realizar las entrevistas utilizando los cuestionarios diseñados en la fase de planeación.
2. Inspeccionar físicamente los lugares.
3. Verificar a través de preguntas adicionales la veracidad de la información recibida.

Análisis de la información:

En esta fase se procede a organizar, tabular y analizar la información recolectada, generando gráficas que permitan comprender de manera más sencilla los diferentes aspectos estudiados.

1. Analizar las cifras de impacto financiero y no financiero para cada uno de los procesos.
2. Analizar los hallazgos por proceso sobre los tiempos y puntos objetivos de recuperación (RTO, RPO) definidos por los entrevistados.
3. Consolidar la información de impactos financieros, no financieros, detenimiento de los procesos y costos asociados a la reposición de los activos destruidos por un posible desastre.

Informe de Resultados:

Una vez recolectada y analizada la información se genera un reporte con los principales hallazgos y observaciones. Mediante el informe del análisis de impacto del negocio se pretende mostrar el resultado que arroja el análisis de la información.

1. Presentar la clasificación de los procesos por el posible impacto financiero.
2. Presentar la clasificación según el impacto no financiero.
3. Presentar consolidados de RTO.
4. Presentar consolidados de RPO.
5. Presentar los activos que tendrán que ser adquiridos (reposición) como consecuencia de un posible desastre.
6. Generar observaciones sobre los resultados obtenidos.
7. Clasificar los procesos por su nivel de criticidad.

3.3.4. Evaluacion de riesgos

El propósito principal de esta fase es conocer cuáles amenazas o riesgos específicos enfrenta GeoVictoria en sus procesos y servicios críticos del negocio, identificados como resultado del análisis de impacto del negocio, con el fin de determinar la forma en que algunos riesgos serán controlados y mitigados a un nivel aceptable según criterios previamente definidos.

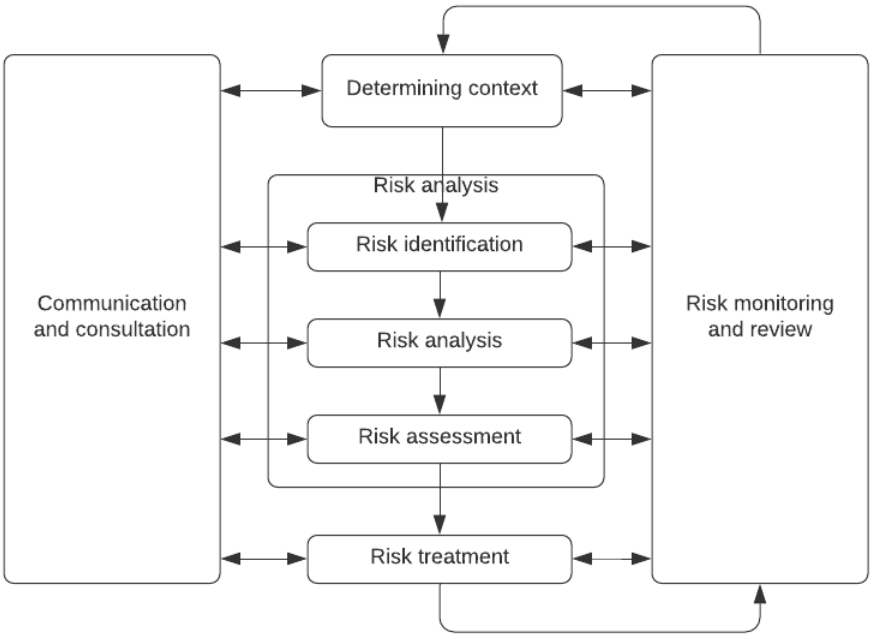


Figura 39 - Proceso de evaluación de riesgos.

Es conveniente mencionar que durante esta fase los riesgos (operativos) se analizarán desde el punto de vista de la continuidad del negocio considerando aspectos cómo personas, servidores, edificios, tecnología, entre otros, sin dejar de lado su relación directa con los procesos determinados como críticos. El tipo de vulnerabilidades y amenazas al que se ven expuestos estos activos varía dependiendo de la naturaleza de los mismos.

Las amenazas y vulnerabilidades que se incluyen para el caso específico del proyecto, serán las relacionadas con la no disponibilidad de los activos asociados a los procesos críticos del negocio. Una parte importante de contar con un plan de continuidad del negocio, es el hecho de realizar una efectiva gestión de riesgo y así evitar las frecuentes activaciones del sitio alterno, actividad que tiene sus propios riesgos, costos y dificultades. En esta etapa, se analizaron las amenazas y vulnerabilidades identificadas previamente, analizando el escenario donde puede materializarse el riesgo de interrupción, así como su origen y las afectaciones potenciales a los activos, el análisis contempló doce escenarios de riesgo que se describen a continuación:

1. Acceso a la edificación: Enumera los controles, los procedimientos y las buenas prácticas que permiten mitigar el riesgo de que personal no autorizado ingrese a las instalaciones y pueda generar daños a los activos de la organización.

2. Administración y entorno tecnológico: Relaciona los hábitos y las buenas prácticas que permiten administrar, asegurar, disponer y controlar los sistemas tecnológicos, de tal forma que estén alineados con los estándares internacionales y regulaciones nacionales en temas de seguridad de la información.
3. Información y administración del edificio: Relaciona procedimientos de seguridad, responsabilidades del personal, cultura y capacitación para responder a incidentes en el edificio.
4. Oficina y estaciones de trabajo: Relaciona las políticas de seguridad de la información definidas por la compañía y las buenas prácticas del personal que aseguren, en el evento de una interrupción del negocio, la disponibilidad, confidencialidad, seguridad e integridad de la información, esto incluye el teletrabajo.
5. Perímetro y estacionamiento: Relaciona los controles, las políticas y los procedimientos que permitan evitar y responder frente a incidentes de seguridad en el perímetro de la compañía.
6. Protección anti-incendios: Relaciona la capacitación del personal, los equipos de extinción y los sistemas de control que permitan responder rápida y eficientemente a un incendio en el edificio y/o en el centro de cómputo.
7. Riesgos entorno geográfico: Relaciona las fuentes latentes de riesgo aledañas a la organización y que puedan generar un potencial riesgo de evento disruptivo.
8. Riesgos naturales: Relaciona los aspectos de ubicación geográfica, climática y del entorno natural que puedan afectar a la empresa.
9. Riesgos potencia eléctrica: Relaciona las políticas, los controles y los procedimientos que permitan asegurar el suministro de energía eléctrica al edificio y equipos críticos, aunque los servicios se encuentran alojados en Microsoft Azure se consideran las instalaciones donde está el personal que administra los sistemas localmente.
10. Riesgos telecomunicaciones: Relaciona las políticas, los controles y los procedimientos que permitan mantener la comunicación (voz y datos) de la organización.

3.3.5. Estrategias de continuidad

La estrategia de continuidad es un mecanismo que permite la recuperación y continuidad de las funciones críticas de una organización frente a un desastre o una interrupción mayor. Son consideradas como estrategias no sólo los recursos y actividades requeridas frente a la interrupción, sino los requeridos para reducir la probabilidad de ocurrencia y el impacto de la interrupción. Para definir las estrategias de continuidades posibles, se debe contar con un entendimiento sobre los siguientes aspectos:

1. Resultados del análisis de impacto del negocio.
2. Tiempos y puntos objetivo de recuperación (RTO y RPO) requeridos para los procesos críticos.
3. Procesos críticos a soportar.

4. Porcentaje aceptable de degradación de la operación del proceso.
5. Aspectos de carácter jurídico que se deben cumplir según la naturaleza del proceso al momento de implementar una estrategia de recuperación.
6. Resultados del análisis de riesgos y las alternativas de tratamiento de riesgo a implementar sobre los activos (tecnológicos e información) asociados a los procesos.
7. Amenazas posibles a los activos (tecnológicos e información) de los procesos.
8. Vulnerabilidades existentes en los activos (tecnológicos e información) de los procesos.

El propósito de esta fase consiste en seleccionar las estrategias de recuperación o continuidad, orientadas a brindarle confiabilidad a los servicios, considerando los resultados del análisis de impacto del negocio, la evaluación de riesgos y la realización de un análisis cuantitativo de los elementos requeridos para la recuperación.

En la siguiente tabla se visualiza la información referente:

Tabla 4 - Estrategias de continuidad

	Posibles escenarios				
	Infraestructura no disponible	TI no disponible	Recurso humano no disponible	Proveedor no disponible	Información no disponible
Amenazas	a. Incendio, inundación, actos de violencia, terremoto. b. Cierre parcial.	a. Falla eléctrica b. Incendio c. Inundación d. Terremoto e. Falla tecnológica de Microsoft Azure	a. Incendio b. Actos de violencia c. Terremoto d. Cierre parcial e. Ausencia, retiro, muerte de un funcionario f. Pandemia	a. Falla Eléctrica b. Incendio c. Inundación d. Terremoto e. Falla tecnológica	a. Falla Eléctrica b. Incendio c. Inundación d. Terremoto o sismo e. Fallas tecnológicas en: comunicaciones, software, bases de datos, almacenes de datos. f. Error humano g. Hurto

Alternativas operativas	a. Teletrabajo b. Valerse de proveedores c. Centro de trabajo alterno	a. Estrategia DRP	a. Definición de la estructura de recuperación en cascada (ERC) b. Capacitación c. Rotación d. Documentación de procedimientos	a. Definir proveedores alternos b. Definir acuerdos de niveles de servicio específicos para *Business Continuity Management*.	a. Respaldo de la información clave del proceso b. Proveedores y/o medios alternos para el servicio de comunicación

Las alternativas operacionales que tiene la empresa, para recuperar la funcionalidad de sus procesos críticos cuando se presente una ausencia de algún recurso clave, después de un evento disruptivo son:

Tabla 5 - Alternativas operacionales.

Evento disruptivo	Amenazas	Alternativas operativas
No disponibilidad de colaboradores del proceso	a. Huelga del personal b. Pandemia c. Intoxicación colectiva d. Indisposición de colaboradores (Ausencia, retiro o muerte)	a. Definición de árboles de llamada b. Capacitación c. Rotación d. Documentación de procedimientos
No disponibilidad de la infraestructura física	a. Incendio b. Inundación c. Actos de Violencia o atentado terrorista d. Sismo o terremoto e. Asonadas f. Fugas de gas g. Explosión	a. Teletrabajo b. Acuerdo con terceros c. Respaldo entre sedes d. Centro de trabajo alterno para procesos administrativos
No disponibilidad de los servicios tecnológicos	a. Falla Eléctrica b. Incendio	a. Estrategia DRP

	c. Inundación d. Sismo o terremoto e. Fallas tecnológicas en: Comunicaciones, software, bases de datos	
No disponibilidad de información	a. Falla Eléctrica b. Incendio c. Inundación d. Sismo o terremoto e. Fallas tecnológicas en: Comunicaciones, software, bases de datos f. Error humano g. Hurto	a. Respaldo de la información clave del proceso b. Proveedores y/o medios alternos para el servicio de comunicación
No disponibilidad de proveedores y/o terceros	a. No disponibilidad del proveedor por eventos propios de su operación: b. Falla Eléctrica c. Incendio d. Inundación e. Huelgas o asonadas f. Pandemias g. Actos de violencia h. Sismo o terremoto i. Fallas tecnológicas j. No disponibilidad de sus proveedores	a. Definir proveedores alternos del servicio b. Definir acuerdos de niveles de servicio específicos para *Business Continuity Management*.

3.3.6. Comité de crisis

El comité de crisis tiene como función principal la toma de decisiones en caso de que ocurra un evento disruptivo que conlleva a la interrupción de los servicios críticos de GeoVictoria.

Entre las funciones principales podemos resaltar las siguientes:

- Analizar la situación para responder oportunamente.
- Tomar la decisión de activar o no el plan de continuidad del negocio.
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.
- Definir un presupuesto estimado para gastos que genere la crisis.
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.
- Tomar decisiones ante situaciones o imprevistos durante la recuperación de operaciones.
- Comunicar a los diferentes comités de la organización las decisiones que se tomen.

Para el caso de GeoVictoria, se propone la creación de un comité de crisis conformado de la siguiente manera:



Figura 40 - Equipos del comité de crisis.

- Equipo Directivo: Avala la decisión tomada por el equipo de manejo de incidentes para la activación del plan de continuidad del negocio. Monitorea el incidente hasta su estabilización y retorno a la normalidad.
- Equipo de Manejo de Incidentes: Verifica el incidente, analiza las consecuencias e impactos potenciales, decide la activación o no del plan de continuidad del negocio y notifica al Equipo Directivo.
- Equipos de Apoyo: Son los equipos necesarios para soportar la ejecución del plan de continuidad del negocio cuando el equipo principal no puede suplir la tarea.
- Equipo de Comunicaciones: Es el responsable del manejo de las comunicaciones con todas las partes interesadas.

3.3.7. Comunicaciones

Las comunicaciones tienen como función principal servir de apoyo para que, en el caso de la ocurrencia de un evento disruptivo, se puede proceder de manera efectiva y eficiente a realizar el contacto entre todo el personal que conforman el comité de crisis.

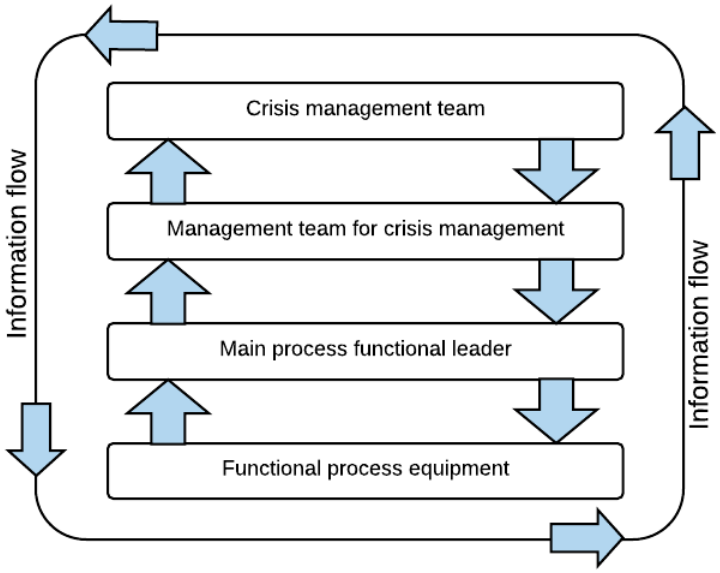


Figura 41 - Comunicación entre equipos del comité de crisis.

Los equipos de comunicaciones son los responsables de la generación y emisión de las comunicaciones corporativas hacia las partes interesadas tanto externas (entes de control, clientes, proveedores) como internas (junta directiva, funcionarios y sus familiares) durante y después de la crisis.

En GeoVictoria, los responsables de las comunicaciones, operarán en contingencia de la siguiente manera:

- Comunicaciones con los organismos de control: El responsable es el vocero oficial de GeoVictoria ante el comité primario.
- Comunicaciones con las entidades externas y medios: La responsable es el área de comunicaciones. Esta comunicación se detalla en el DRP en el capítulo anterior con el árbol de llamadas.
- Comunicaciones con los funcionarios: El responsable es el líder de talento humano hacia los colaboradores y sus familias y líder de gestión de la contratación para los contratistas. Los elementos con los que cuenta este equipo para comunicarse internamente se detallan en el DRP en el capítulo anterior con el árbol de llamadas.