1. Propósito

El presente Plan de Continuidad del Negocio tiene como finalidad asegurar la continuidad y el restablecimiento de los procesos y servicios críticos de G&S, de frente a diversos eventos disruptivos de origen natural y causados por el hombre.

2. Alcance

Este Plan será aplicable a la Oficina de G&S ubicada en Av. Del Ejército Nro.250 - Miraflores.
El Plan de continuidad considera los incidentes que se pueden generar por los diferentes tipos de eventos considerados en la Matriz de análisis riesgo impacto – negocio, estos son: Terremotos/ maremotos, robo a la oficina, ataques cibernéticos, epidemias/ pandemias, golpe de estado, huelgas/ ausentismo y caída del proveedor.

3. Objetivos

- Mantener el funcionamiento de los procesos esenciales y mínimos básicos de G&S.
- Proteger al personal de G&S ante los efectos de un evento disruptivo.
- Asegurar la disponibilidad de los equipos informáticos necesarios para la continuidad del servicio.
- Proteger la información vital para G&S.
- Cumplir con los tiempos estimados de recuperación para las diferentes áreas críticas.

4. Roles y responsabilidades del equipo

La responsabilidad de la ejecución de este plan recaerá en la Gerencia de línea.

5. Definiciones

Se definen los siguientes términos:

Comité de Continuidad de Negocio (CN): Son los responsables de coordinar e implementar la estrategia de G&S de acuerdo con los pasos sugeridos en este Plan, supervisan la implementación del Plan durante un evento disruptivo, recopilan información para determinar el impacto y sus consecuencias para las operaciones de la instalación y recomiendan la acción de continuidad del negocio al Gerente de línea y/o Gerente de operaciones.

Tiempo Objetivo de Recuperación (TOR): El Tiempo Objetivo de Recuperación es el tiempo transcurrido entre la interrupción del proceso y el punto en el cual éste debe estar totalmente operativo.

Tolerancia Máxima Periodo de Disrupción (TMPD) / Máxima Parada Aceptable (MPA): Tiempo máximo permitido en el que los procesos o servicios críticos están indispuestos, si se sobrepasa este tiempo, producirá un impacto inaceptable del servicio.

Punto objetivo de recuperación (RPO): Cantidad máxima aceptable de pérdida de datos después de un incidente imprevisto expresada en tiempo

Condición mínima de operación (MBCO): Mínimo nivel de productos y/o servicios que es aceptable, para que la organización alcance sus objetivos de negocio durante una interrupción

Servicio crítico: Servicio que tiene relevancia sobre los demás, debido a su impacto económico en la organización.
Proceso crítico: Proceso que es vital para las actividades comerciales de la organización.
Recurso crítico: Recurso que es imprescindible para mantener operativo un proceso o servicio crítico.
Personal crítico: Personal que es esencial para mantener continuo un proceso crítico.

6. Plan de continuidad de negocio

Entre las acciones seleccionadas para mantener la continuidad del negocio se cuenta con:

- **Acuerdos con proveedores,** Que cuenten con disponibilidad para asegurar las funciones críticas.
- **Acuerdos de servicios, pagos vía electrónica:** Estos compromisos están orientados a la provisión de servicios para asegurar la operación de la oficina en caso sea necesario asistir. Entre ellos, se tienen los pagos a través de internet y servicio de internet.
- **Centro de operaciones:** El lugar seleccionado es la sala de reuniones de la oficina y/o videoconferencia. En esta reunión se coordinará las acciones de respuesta y recuperación ante eventos adversos. En caso se produzca un daño severo a las instalaciones de la oficina, se ha considerado como lugar alternativo, los domicilios de cada personal y continuar las operaciones y coordinaciones de manera remota.
- **Reutilización de recursos:** Reubicación de personal con funciones no urgentes en tareas que requieren una mayor prioridad. Para ello se cuenta con procesos claramente establecidos y difundidos y el personal se encuentra capacitado.
- **Trabajo a distancia remoto:** Trabajo a distancia del personal desde sus domicilios vía internet preferentemente. Se cuenta con acceso a los archivos digitales de los contratos y órdenes de compras, file de personal y de otros documentos importantes necesarios para mantener la operación de la oficina.

7. Organización de responsables del Plan

7.1. Miembros del Comité de continuidad del negocio

Tienen como responsabilidad el Gerente de Línea realizar el análisis de situación para decidir o no la activación del Plan de continuidad, iniciar la cadena de llamadas en caso de activación del plan, tomar decisiones para la continuidad y recuperación de los servicios críticos, así como hacer el seguimiento de las actividades de respuesta y recuperación implementadas.

N.º	Miembros	Reemplazo
1	Gabriel Quiroz	Rubén Parodi
2	Micaela Bravo	Jessica Zavaleta
3	Deisy Verde	María Flores
4	Paolo Reategui	Andre Zegarra

7.2. Responsables de comunicaciones

Esta persona está encargada de las comunicaciones internas, externas y relacionamiento con autoridades; así como la información al personal involucrado sobre el evento y las acciones implementadas.

N°	Titular Responsable de Comunicaciones	Reemplazo
1	Deisy Verde	María Flores

7.3. Responsable de la logística y recursos

Es responsable de la atención de las necesidades logísticas para la implementación de las acciones de respuesta y la recuperación, lo cual incluye servicios generales, transporte, correspondencia, apoyo secretarial y dotación de materiales. Este equipo apoya a los otros para asegurar la efectiva respuesta ante la ocurrencia de eventos adversos.

N°	Titular Responsable	Reemplazo
1	Gabriel Quiroz	Rubén Parodi

7.4. Responsable de recuperación de la información

Es responsable de la recuperación efectiva de los sistemas informáticos y administrativos de la Oficina con énfasis en los procesos de ejecución del servicio, compras, recursos humanos y finanzas.

N°	Titular Responsable	Reemplazo
1	Paolo Reategui	André Zegarra

7.5. Brigada de Seguridad y Salud en el Trabajo

Estos equipos realizan el control de eventos puntuales e incidentes al interior de la Oficina y que no superan la capacidad de respuesta. La brigada de seguridad y salud en el trabajo se encarga de temas referentes a Primeros auxilios, Seguridad y Evacuación.

8. Determinación de los procesos, recursos y servicios críticos

Proceso	¿Es crítico?	Justificación	Personal crítico	Personal de reemplazo
Gestión Comercial	Sí	Proceso que tiene como objetivo la generación y cierre de oportunidades comerciales para la organización.	Ejecutivos Comerciales	Validar la cantidad de personal interno disponible posterior al proceso afectado. De no contar con el personal interno disponible, el externo debe alinearse al Perfil de puesto – Ejecutivo Comercial Jr.
Gestión de Incidentes y peticiones	SÍ	Proceso que tiene como objetivo la atención de casos solicitados por los clientes de la organización.	Consultores y Especialistas	Validar la cantidad de personal interno disponible posterior al proceso afectado. De no contar con el personal interno disponible, el externo debe alinearse al Perfil de puesto – Consultor
Gestión de la disponibilidad y continuidad (*) (*) Toma en cuenta el proceso de disponibilidad	Sí	Proceso que tiene como objetivo de que todos los sistemas, servicios y recursos estén dentro de los SLA´s establecidos con el cliente para mantener la eficiencia y productividad requerida.	Consultores y Especialistas	Validar la cantidad de personal interno disponible posterior al proceso afectado. De no contar con el personal interno disponible, el externo debe alinearse al Perfil de puesto – Consultor o Gestor de servicio.

Proceso Gestión Comercial

Recurso	¿Es crítico?	Justificación	Condición mínima de operación (MBCO)
Personal	Sí	Personal que se encarga de lograr nuevas oportunidades y fidelizar al cliente de G&S.	Se puede operar como mínimo con 1 Ejecutivo Comercial
Infraestructura	No	No es necesario el trabajo en sede ya que todo se encuentra alojado en nube y se realiza trabajo remoto.	N/A
Equipos informáticos y de telecomunicaciones	Sí	Se necesita de una laptop para realizar sus actividades.	Se debe contar por lo menos con 01 laptop para trabajos en sede y/o 01 laptop para el trabajo remoto.
Software	No	El seguimiento a sus oportunidades se puede realizar mediante una agenda o Excel de seguimiento.	N/A
Insumos de oficina	No	No es necesario algún insumo de oficina ya que se puede realizar el trabajo de manera remota.	N/A
Registros imprescindibles	No	No se cuenta con registros imprescindibles que detengan la operación comercial.	N/A
Proveedores/ Servicios de TI	No	No se depende de ningún proveedor para realizar alguna actividad relacionada al logro de oportunidades.	N/A

Proceso Gestión de incidentes y peticiones

Recurso	¿Es crítico?	Justificación	Condición mínima de operación (MBCO)
Personal	Sí	Es necesario el personal para la atención de los casos de los clientes.	Se puede operar como mínimo con 2 consultores.
Infraestructura	No	No es necesario el trabajo en sede ya que todo se encuentra alojado en nube y se realiza trabajo remoto.	N/A
Equipos informáticos y de telecomunicaciones	Sí	Se necesita de una laptop para realizar sus actividades.	Se debe contar por lo menos con 02 laptops para trabajos en sede y/o 02 laptops para el trabajo remoto.
Software	No	El personal tiene la opción de manejar el seguimiento mediante correos para el cumplimiento de los servicios.	N/A

Insumos de oficina	No	No es necesario algún insumo de oficina ya que se puede realizar el trabajo de manera remota.	N/A
Registros imprescindibles	No	Los registros de los casos se llevan a través del Sistema de gestión de tickets o correo.	N/A
Proveedores/ Servicios de TI	No	No se necesita de un proveedor para realizar las actividades relacionadas a la atención de un caso.	N/A

Proceso Gestión de Disponibilidad y Continuidad

Recurso	¿Es crítico?	Justificación	Condición mínima de operación (MBCO)
Personal	Sí	Es necesario a los consultores y especialistas para cumplir con los servicios pactados con el cliente.	Se puede operar como mínimo con 2 consultores.
Infraestructura	No	No es necesario el trabajo en sede ya que todo se encuentra alojado en nube y se realiza trabajo remoto.	N/A
Equipos informáticos y de telecomunicaciones	Sí	Se necesita de una laptop para realizar sus actividades.	Se debe contar por lo menos con 02 laptops para trabajos en sede y/o 02 laptops para el trabajo remoto.
Software	No	El personal maneja el seguimiento de los casos mediante los correos y el registro en excel para el cumplimiento de los servicios.	N/A
Insumos de oficina	No	No es necesario algún insumo de oficina ya que se puede realizar el trabajo de manera remota.	N/A
Registros imprescindibles	No	Los registros de los casos se llevan a través del Sistema de gestión de tickets o correo.	N/A
Proveedores/ Servicios de TI	No	La caída de disponibilidad del servicio del proveedor de Microsoft no son críticos para continuar brindando el servicio al cliente.	N/A

8.1. Determinación y análisis de servicios críticos

Servicio	Justificación de la criticidad	MBCO*	TOR*	RPO*	MTPD*
Cloud Hosting (ESTÁNDAR)	58% del total de la facturación anual de la línea	>=95.5% 41596 minutos disponibles del sistema **(*) Para activar el plan verificar si el servicio tiene SLA ´s específicos.**	48 horas **(*) El Tiempo objetivo para que el servicio vuelva a la normalidad.** **Menor que MTPD ya que luego de eso pierdo a mi cliente**	1 día **(*) Tiempo que se puede soportar ante una pérdida de información.**	3 meses **(*) Tiempo máximo para no perder al cliente.**
Asignación Fija	22% del total de la facturación anual de la línea	2 consultores **(*) Cantidad de consultores que están bajo asignación fija**	1 día **(*) Tiempo máximo para poder reemplazar a los consultores.**	N/A	1 semana **(*) Tiempo máximo al estar por debajo del MBCO para no perder al cliente.**

9. Determinación de eventos disruptivos

Evento disruptivo	Recursos afectados	Servicios afectados
Terremoto/ Maremoto	Consultores/ Especialistas Laptops	Asignación fija
Robo a la oficina	Laptops (información)	N/A
Ataque cibernético	Sistemas (SIGAD y SGT) Microsoft proveedor	Cloud hosting
Epidemias/ Pandemias	Consultores/ Especialistas	Asignación fija
Golpe de estado	Consultores/ Especialistas	Asignación fija
Huelgas o Ausentismo	Consultores/ Especialistas	Asignación fija
Caída de proveedor	Microsoft proveedor	Cloud hosting

10. Activación del plan de respuesta de emergencias

El Plan de continuidad se activará solo en los casos en que un evento disruptivo afecte a los procesos y servicios críticos y no se pueda recuperar con actividades de gestión interna o servicios hasta por debajo de su condición mínima de operación (MBCO), la activación será realizada por el Gerente de línea o Gerente de operaciones.

11.Respuesta ante emergencias

El Plan de respuesta ante emergencias define las actividades antes y durante un evento disruptivo. A continuación, el detalle:

a) Terremoto/ Maremoto

Afectación

Dependiendo del grado de magnitud del terremoto puede causar que se caigan las paredes más débiles o puede significar la destrucción completa de la oficina:

- Indisponibilidad de consultores/ especialistas y equipos informáticos (laptops) como resultado de un terremoto
- Afectación del servicio de asignación fija, como resultado de un terremoto

Acción

Antes

N°	Actividad	Responsable
1	Definir brigada de emergencia en caso se encuentre se encuentre en sede.	Jefe de RRHH
2	Contar con señalización y equipamiento correspondiente en sede.	Jefe de Administración
3	Capacitación y concientización a las brigadas y el personal interno.	Jefe de RRHH
4	Definir personal crítico y de reemplazo.	Gerente de Infraestructura & Cloud

Durante

N°	Actividad	Responsable
1	Independientemente del grado o magnitud del terremoto la acción por parte del brigadista encargado es de ayudar a otros a evacuar el edificio evitando pérdidas humanas y de ser posible de los equipos informáticos portátiles	Brigadistas
2	El medio de comunicación recomendado son los mensajes de texto ya que las líneas de llamadas se encontrarán sobrecargadas.	Todo el personal
3	Identificar al personal que haya resultado afectado.	Jefe de RRHH

Después

N°	Actividad	Responsable
1	Una vez que se ha garantizado la seguridad de todo el personal, es importante validar la disponibilidad del personal crítico.	Gestores de Servicios / Gerente de Línea
2	De no contar con el personal crítico interno disponible para mantener las operaciones, se deberá contactar a proveedores externos.	Gestores de Servicios / Gerente de Línea
3	En caso sea necesario, evaluar grado de impacto y viabilidad de la infraestructura de las oficinas y de su equipamiento.	Gerente de Operaciones Jefe de Administración
4	Si las casas de los trabajadores no viables conforme al impacto del terremoto, se establecerá acuerdos con Cabinas con accesos / Contrato con workplace.	Gerente de Operaciones Jefe de Administración
5	Gestionar la accesibilidad del personal a los servidores virtuales de la empresa.	Administrador de Soporte
6	Para los casos en los cuales haya pérdida de información, realizar la recuperación de backup.	Administrador de Soporte
7	Validar si el gobierno ha establecido algún lineamiento normativo a cumplir y proceder a su implementación	Jefe de RRHH/ Responsable del SIG

b) Robo a la oficina

Afectación

El robo de equipos a los miembros de la empresa, por lo general los gestores o consultores son personal que actúa en los procesos principales de la línea, en este caso la afectación recae severamente por la información de los clientes que posee el personal en la laptop o equipo a su cargo.

- Indisponibilidad de equipos informáticos (laptops) y su información como resultado de un robo de oficina.

Acción

Antes

N°	Actividad	Responsable
1	Verificar el funcionamiento de las cámaras de seguridad de la empresa	Jefe de Administración
2	Todo ingreso a sede se debe comunicar al área de Administración	Jefe de Administración
3	Los equipos deben contar con contraseña para poder ingresar a su sesión	Administrador de Soporte

Durante

N°	Actividad	Responsable
1	Durante el evento del robo no se debe poner resistencia.	Todo el personal
2	Utilizar canales de comunicación inmediatos (whatsapp, llamadas, mensajes a través de teléfono móvil) respecto al evento a su jefatura directa.	Todo el personal

Después

N°	Actividad	Responsable
1	Poner en aviso a la policía nacional y poner la denuncia en la comisaria más cercana.	Personal afectado
2	Validar si hubo afectación o robo de equipos críticos, esto incluye determinar qué datos críticos se han perdido y que sistemas se ven afectados.	Administrador de Soporte
3	Realizar la recuperación de datos de los respaldos de información disponibles y/o el reemplazo de los equipos críticos para mantener las operaciones en mantenimiento.	Administrador de Soporte

c) Ataque cibernético

Afectación

Al estar bajo un ataque cibernético se vulneraría la información de la empresa y la información de clientes a los cuales se les ha realizado un servicio se pone en riesgo no solo a G&S si no a los clientes, lo que generaría desconfianza y pérdida de clientes.

- Indisponibilidad del proveedor Microsoft, del sistema SIGAD y SGT como resultado de un ataque informático.
- Afectación del servicio de Cloud Hosting si hay un ataque al proveedor y hacia el servicio soporte cloud y bolsa de horas si afecta a sistemas internos como SIGAD y SGT.

Acción

Antes

N°	Actividad	Responsable
1	Implementar un firewall u otros sistemas para prevenir y detectar ataques informáticos.	Administrador de Soporte
2	Contar con un modelo de speech para la comunicación de eventos disruptivos hacia los usuarios y clientes.	Gestores de Servicios y Administradores de Soporte
3	Validar que las copias de seguridad se encuentren activadas.	Administrador de Soporte
4	Difusiones al personal sobre cómo identificar o proceder ante un ataque cibernético.	Procesos y Certificaciones / Administrador de Soporte

Durante

N°	Actividad	Responsable
1	Comprobar y verificar el tipo de ciberataque.	Administrador de Soporte
2	En caso las acciones para prevenir y detectar los ataques informáticos no hayan sido suficientes, alertar sobre el ciberataque que se propaga en la red de G&S.	Equipo de Procesos y Certificaciones / Administrador de Soporte
3	En caso no se contenga el ataque cibernético, desconectar de la red todos los componentes tecnológicos.	Administrador de Soporte / Gerente de Infraestructura & Cloud
4	Comunicar a las partes interesadas (clientes, proveedores, etc) respecto al evento disruptivo por el medio disponible (Correos, whatsApp, llamadas, mensajes a través de teléfono móvil), en caso sea por correo se recomienda activar el acuse de recibido.	Gestores de Servicios

Después

N°	Actividad	Responsable
1	Restaurar sistemas desde los respaldos seguros y no afectados por el ataque.	Administrador de Soporte
2	Dar parte a la policía - División de Investigación de Delitos de Alta Tecnología (DIVINDAT) si el caso aplica.	Administrador de Soporte / Gestores de Servicios
3	Verificar que el Ciberataque ha sido contenido y los servicios afectados vuelvan a Producción.	Administrador de Soporte
4	Realizar un informe del incidente ocurrido a las partes interesadas.	Administrador de Soporte / Gestores de Servicios
5	Identificar y tomar medidas para solucionar las vulnerabilidades del ataque.	Administrador de Soporte

d) Epidemias/ Pandemias

Afectación

Esta situación es crítica y puede significar daño a la salud de nuestro personal inclusive la muerte.

- Indisponibilidad de consultores/ especialistas como resultado de una epidemia/pandemia
- Afectación del servicio de asignación fija, como resultado de la indisponibilidad del personal.

Acción

Antes

N°	Actividad	Responsable
1	Contar con un médico ocupacional que asesore a la organización.	Jefe de RRHH
2	Contar con charlas respecto a la salud en el trabajo.	Jefe de RRHH
3	Definir personal crítico y reemplazo.	Gerente de Infraestructura & Cloud

Durante

N°	Actividad	Responsable
1	Comunicar a las partes interesadas respecto al evento disruptivo y las acciones a tomar por el medio disponible (WhatsApp, llamadas, correo, mensajes a través de teléfono móvil), en caso sea por correo se recomienda activar el acuse de recibido.	Jefe de RRHH
2	Establecer trabajo 100% remoto.	Jefe de RRHH Directorio.
3	Implementar protocolos de protección a la integridad y salud de los colaboradores.	Jefe de RRHH

Después

N°	Actividad	Responsable
1	Establecer mecanismos de detección y monitoreo del estado de salud de los colaboradores.	Jefe de RRHH, Médico Ocupacional
2	Identificar al personal que haya resultado afectado	Jefe de RRHH Médico Ocupacional
3	Una vez que se ha garantizado la seguridad y salud de todo el personal, es importante validar la disponibilidad del personal crítico.	Gestores de Servicios / Gerente de Línea
4	De no contar con el personal crítico interno disponible para mantener las operaciones, será necesario contactar a proveedores externos.	Gestores de Servicios / Gerente de Línea

e) Golpe de estado

Afectación

Un golpe de estado puede significar una crisis política y social que puede poner en riesgo la integridad física de nuestros colaboradores.

- Indisponibilidad de consultores/ especialistas como resultado de un golpe de estado.
- Afectación del servicio de asignación fija, como resultado de la indisponibilidad de consultores/ especialistas.

Acción

Antes

N°	Actividad	Responsable
1	Definir reuniones periódicas de las Gerencias de línea y miembro de directorio respecto al desarrollo del negocio y operaciones.	Jefe de RRHH/ Gerencia de Línea/ Miembros de directorio.
2	Definir personal crítico y remplazo.	Gerente de Infraestructura & Cloud

Durante

N°	Actividad	Responsable
1	Comunicar a las partes interesadas respecto al evento disruptivo y las acciones a tomar por el medio disponible (WhatsApp, llamadas, correo, mensajes a través de teléfono móvil), en caso sea por correo se recomienda activar el acuse de recibido.	Jefe de RRHH
2	Establecer trabajo 100% remoto.	Jefe de RRHH
3	Asegurar el número de personal crítico para la operatividad del negocio.	Gestores de Servicios / Gerente de Línea
4	De no contar con el personal crítico interno disponible para mantener las operaciones, se deberá contactar a proveedores externos.	Gestores de Servicios / Gerente de Línea

Después

N°	Actividad	Responsable
1	En las reuniones de seguimiento se evaluará el grado del evento con una revisión detallada de todo el alcance y se determinará en que afectará a la organización a futuro, se considerarán diversos escenarios posibles y se evalúa proponer acciones mitigantes específicas que ayude a prepararse y responder de manera efectiva.	Jefe de RRHH, Gerencia General y Directorio

f) Huelgas o Ausentismo

Afectación

Una huelga o ausentismo, aunque tenga un nivel de probabilidad baja, puede afectar el servicio que brinda G&S.

- Indisponibilidad de consultores/ especialistas como resultado de una huelga o ausentismo.
- Afectación del servicio de asignación fija, como resultado de la indisponibilidad de consultores/ especialistas.

Acción

Antes

N°	Actividad	Responsable
1	Se debe contar con un registro de los consultores externos con los que se ha trabajado para que sea compartido con las partes involucradas en caso de esta situación.	Gerente de Infraestructura & Cloud / Responsable del SIG
2	Definir personal crítico y remplazo.	Gerente de Infraestructura & Cloud

Durante

N°	Actividad	Responsable
1	La persona que detecte el ausentismo debe informar a los responsables de la línea afectada por el medio disponible, en caso sea por correo se recomienda activar el acuse de recibido.	Gerente de Infraestructura & Cloud
2	Un responsable de la línea deberá comunicarse con los consultores externos que se encuentran dentro del registro, para cubrir las horas necesarias determinadas por el Gerente de línea.	Gestores de Servicios / Gerente de Infraestructura & Cloud

Después

N°	Actividad	Responsable
1	Se deberá realizar un monitoreo a los nuevos consultores externos para verificar que se cumplen con los SLA y otros requisitos del servicio.	Gerente de Infraestructura & Cloud
2	Notificar los cambios a las partes interesadas sobre los consultores que ingresan a laborar.	Gestores de Servicios / Gerente de Infraestructura & Cloud

g) Caída de proveedor

Afectación

En caso el proveedor/ partner de G&S sufra una caída imprevista o no se encuentren disponibles los servicios acordados según contrato con G&S; los servicios acordados en los contratos con clientes se verían afectado y generarían penalidades y en el peor de los casos la pérdida del cliente afectando el prestigio de la empresa.

- Indisponibilidad de Microsoft como resultado a la caída del proveedor.
- Afectación del servicio cloud hosting, como resultado a la caída del proveedor.

Acción

Antes:

N°	Actividad	Responsable
1	Contar con alertas de disponibilidad de componentes alojados en nube.	Gerente de Infraestructura & Cloud
2	Establecer contractualmente SLA´s de disponibilidad con el proveedor	Gestores de Servicios / Gerente de Infraestructura & Cloud

Durante:

N°	Actividad	Responsable
1	Comunicar a las partes interesadas respecto al evento disruptivo y las acciones a tomar por el medio disponible (WhatsApp, llamadas, correo, mensajes a través de teléfono móvil), en caso sea por correo se recomienda activar el acuse de recibido.	Gestores de Servicios / Gerente de Infraestructura & Cloud
2	Seguimiento de los sistemas afectados a través de la plataforma del proveedor.	Gestores de Servicios / Gerente de Infraestructura & Cloud

Después:

N°	Actividad	Responsable
1	Se envía un comunicado general a los clientes respecto al inconveniente ocurrido y la solución que brindó el proveedor a través de su portal.	Gestores de Servicios / Gerente de Infraestructura & Cloud

10. Recuperación

SITUACIÓN	EVENTO GENERADOR	ACTIVIDADES DE RECUPERACION
Restricción total o parcial de instalación, equipos y mobiliario para el trabajo del personal.	Robo a la oficina Terremoto, maremoto	1. Comité de CN inicia la evaluación de daños y determina necesidades urgentes para recuperación de servicios críticos. 2. En base al Informe del estado actual de la infraestructura y equipamiento (para terremoto), establecer las acciones para la recuperación de la infraestructura y equipamiento crítico. 3. En base al Informe de perdidas físicas y de información (Robo en oficina), proponer acciones para adquirir nueva infraestructura, o asignación de equipos o reestablecer las copias de seguridad más convenientes. Responsable: Administración. 4. Gerente de operaciones autoriza las compras y contrataciones urgentes (nueva sede según aplique). 5. Evaluar la necesidad de contratar personal para recuperar el nivel de servicio. 6. Coordinación con los proveedores de TI para reestablecer los servicios. 7. Revisar y ajustar los MBCO, TMPD, TOR y RPO.
Restricción a sistemas internos deInformación.	Ataque cibernético	1. Comité de CN evalúa el alcance del ataque e informa a la Gerencia de línea. 2. Tienen atención prioritaria los equipos informáticos de procesos esenciales y mínimo básico. 3. Se ejecutan análisis de vulnerabilidades para la mitigación de riesgos y garantizar la continuidad de las operaciones de la organización. 4. Revisar y ajustar los MBCO, TMPD, TOR y RPO.

Indisponibilidad total o parcial del personal.	Epidemias, Pandemias Huelga y ausentismo Terremoto, maremoto Golpe de estado	1. La Gerencia de Línea/ Comité de Continuidad revisa el personal indisponible ante este evento disruptivo. 2. Activación de proceso de selección de personal en la modalidad de terceros. 3. Realizar contratación de personal para cubrir los puestos que se han desocupado. 4. Priorizar y realizar seguimiento al cumplimiento de los niveles de servicio. 5. Revisar y ajustar los MBCO, TMPD, TOR y RPO.
Restricción total o parcial de los servicios ofrecidos.	Caída del Proveedor	1. Comité de CN junto a partes interesadas evalúa el alcance de la caída e informa a la Gerencia Línea. 2. Seguimiento del problema en la plataforma del proveedor. 3. Restaurar el servicio según los SLA´s establecidos inicialmente con el cliente. 4. Emisión de informe respecto a la caída a las partes interesadas. 5. Revisar y ajustar los MBCO, TMPD, TOR y RPO.

11. Regreso a la normalidad

Luego de atendida la contingencia y recuperados los servicios críticos de G&S, los miembros del Comité de CN evalúan la situación y determinan si procede o no finalizar la activación del Plan de continuidad del negocio. En caso se finalice la activación del plan se procederá con las siguientes acciones:

1. El Comité de CN y/o miembros involucrados preparan un informe, correos u otro medio de evidencias, etc de los efectos del evento. Se debe contar con una evaluación de los daños en las instalaciones y los equipos en caso aplique. Además, se valorará la afectación física o mental del personal a través del servicio médico bajo el ámbito de la cobertura del seguro médico en caso aplique.
2. El Gerente de Operaciones determina la necesidad de reparaciones, compra de nuevos equipos, mobiliario y otros bienes a ser repuestos en caso aplique.

Luego de una crisis se debe velar por la reconstitución de las instalaciones de G&S como lugar de trabajo con condiciones adecuadas. Las operaciones de reconstitución pueden incluir acciones para restablecer

la instalación original o adquirir/arrendar una nueva. Dependiendo del escenario, puede ser necesario relocalizar las operaciones a otro sitio.

12. Prueba del Plan

Las finalidades principales de probar y capacitar el Plan de continuidad son las siguientes:

- Mejorar la capacidad de respuesta de las unidades organizacionales, áreas de trabajo e individuos.
- Familiarizar a todo el personal, particularmente a los directamente involucrados en la implementación del Plan de Continuidad, con los temas o problemas identificados durante una emergencia o riesgo.
- Validar planes, normas, procedimientos y sistemas.
- Identificar deficiencias y corregirlas.
- Mantener/poner al día el Plan.

El ejercicio de prueba (ensayo) está orientado a identificar debilidades del sistema y sugerir acciones correctivas para mejorar la respuesta. Una vez realizados los ejercicios, se complementarán en un informe o correo detallado las lecciones aprendidas, las que serán incorporadas e implementadas según sea necesario.

- Ejercicios en la línea de Infraestructura & Cloud según lo establecido en el Programa de simulacros– implementación de acciones del Plan de continuidad a nivel de la línea.
- Ejercicios para eventos que requieran respuesta técnica se darán periódicamente y se realizará la implementación regular de procesos y servicios que hayan fallado.

Los tipos de ejercicios que se pueden realizar, según aplique, son los siguientes:

Ejercicios	Descripción	Periodicidad
De escritorio	Consiste en realizar un ejercicio en un ambiente “sin estrés”. Para ello, cada representante de rol se sienta alrededor de una mesa de trabajo, y sigue exclusivamente las actividades de su respectivo plan, sin improvisar; cualquier necesidad no documentada debe anotarse como una mejora al plan. Este tipo de ejercicio es útil para validar el uso del documento del plan por parte del personal, para validar incoherencias entre actividades de diferentes roles y para que el personal se familiarice con el documento del plan.	Anual
Parcial	Según cada módulo o rol, consiste en ejercitar el plan de un departamento específico y evaluar si técnicamente el plan es viable, si las actividades son técnicamente correctas, si los tiempos considerados son adecuados o si los RTOs son muy exigentes. Evalúa también si el personal alterno conoce bien las actividades del día – día que son necesarias en el plan.	Anual
Simulación	Es un ejercicio de mayor alcance y complejidad, lo más cercano a la realidad, pero sin afectar la operación diaria ni involucrar el ambiente de producción de tecnología, por lo que debe realizarse en un ambiente controlado para no	Anual

	interrumpir las operaciones. Se puede resumir en “Probar todo como si fuera real, sin afectar el día – día”.	
Escala completa	Es el ejercicio de mayor alcance y complejidad, lo más cercano a un desastre real. A diferencia de todos los tipos anteriores, sí afecta la operación diaria con condiciones de estrés reales, con múltiples departamentos trabajando entre sí y, de ser necesario, considerando viajes y desplazamientos reales. Se puede resumir en “Es un desastre real generado en un ambiente controlado”	Cada 2 años

Programa de simulacros

Se ha definido un “Programa de simulacros” para el desarrollo de los diferentes eventos disruptivos identificados que considere la periodicidad para cada tipo de evento.

Las pruebas pueden ser uno o combinar varios escenarios del negocio. Para la programación de los simulacros se cuenta con un formato el cual se tiene la siguiente información:

- **Responsable:** Área o persona responsable de la ejecución del simulacro
- **Tipo de Simulacro:** Evento disruptivo
- **Periodicidad:** Frecuencia en la cual se ejecutará los simulacros.
- **Objetivo:** Meta que se pretende lograr.

Posterior a la ejecución de cada ejercicio de simulacro, se deberá notificar al Comité de CN para garantizar una respuesta organizada y eficiente ante cualquier situación de emergencia que pueda presentarse.

13. Evaluación de eficacia del Plan

Se realizará la evaluación de este plan cada 2 años o ante algún cambio relevante, utilizando el formato Evaluación del Plan de Continuidad, este documento es elaborado por una persona designada por la Gerencia de línea y aprobada por un miembro de Alta Dirección.

14. Revisión y actualización del Plan

El Plan de continuidad se revisará y actualizará de ser necesario cada 2 años y estos resultados serán presentados en la revisión por la Dirección.

G&S gestión y sistemas	**PLAN DE CONTINUIDAD DEL NEGOCIO**	**Código: G&S-CN-FO-02**
		Versión: v05
		Fecha: 23/04/2024

Control de Cambios			
Versión	**Aprobador**	**Fecha**	**Motivo**
01	Gerente de Línea	04/11/2021	Primera versión del documento
02	Gerente de Línea	29/08/2022	Se mantiene el formato y se agrega a su contenido el evento disruptivo caída de proveedor.
03	Gerente de Línea	25/07/2023	Se actualiza el Comité de CN. Se determinan procesos y recursos críticos. Se adicionan indicadores para el análisis de los servicios críticos.
04	Gerente de Línea	10/10/2023	Se actualiza el Comité de CN y se detallan actividades antes, durante y después de un evento disruptivo.
05	Gerente de Línea	23/04/2024	Se adiciona la instrucción de notificar al Comité de Continuidad después de la ejecución de cada simulacro realizado.

Revisiones y Aprobaciones					
Nombre	**Cargo**	**E**	**R**	**A**	**Firma**
Jessica Zavaleta	Jefa de Procesos y Compliance	X			Ok
Comité de Continuidad de Negocio	Comité de Continuidad de Negocio		X		Ok
Gabriel Quiroz	Gerente de Línea			X	Ok

E: Elaborador

R: Revisor

A: Aprobador