	PLAN DE CONTINUIDAD DEL NEGOCIO	Código: DOC.GE.08
		Actualización: 11 DIC 2019
		Versión: 02
		Página 1 de 7

1. OBJETIVO

Establecer las actividades a realizar para garantizar la continuidad de negocio ante situaciones de sabotaje y ciber ataques, caída de servicios de internet y fallas en las comunicaciones, pérdida de información, cortes de energía, desastres naturales e incendios.

2. ALCANCE

Abarca todas las actividades que garantizan que las operaciones continúen a pesar de una contingencia, que corresponden al plan de continuidad de negocio BCP y las actividades del plan de recuperación de desastres DRP de los procesos de infraestructura de TI. Este plan es aplicable para el administrador de las redes de la compañía y para empleados y contratistas.

2.1. PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS DRP

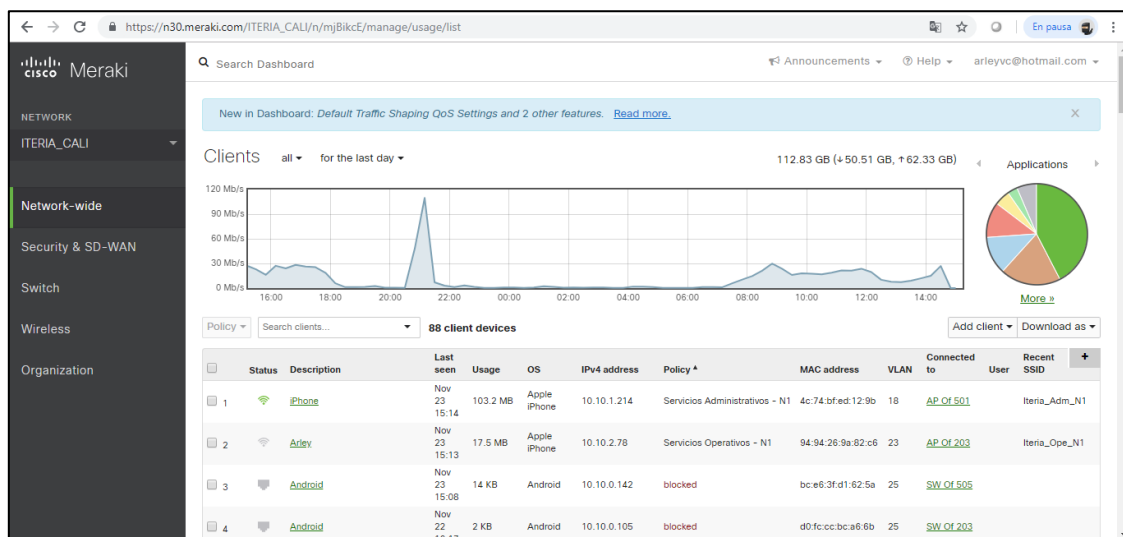
2.1.1. Prevención de sabotaje y ciber ataques desde la red local [LAN]


Se cuenta con una red cableada a la cual se pueden conectar los usuarios y en cada oficina se cuenta con tres Access point, los cuales tiene capacidad para 500 usuarios concurrentes para evitar pérdidas de señal o saturación del canal en las bandas 2.4 y 5 GHz.

De igual forma se cuenta con un sistema de seguridad y trazabilidad de la red (CISCO MERAKI), **Ver gráfico 1**, el cual dispara alertas en caso de que se alcance un 70% de saturación del canal para revisar que dispositivo está consumiendo más ancho de banda.

Así como la distribución en equipos de trabajo de acuerdo al área de trabajo, lo que nos permite darle un porcentaje de ancho de banda de acuerdo a la necesidad.

Gráfico 1



	PLAN DE CONTINUIDAD DEL NEGOCIO	Código: DOC.GE.08
		Actualización: 11 DIC 2019
		Versión: 02
		Página 2 de 7

2.2. Plan de recuperación ante caída de *servicios de internet y fallas en las comunicaciones.*

El operador que tenemos garantiza un 99% en el servicio, en caso de que llegase a presentar alguna incidencia, el plan alterno que tenemos, en orden de aplicación es el siguiente:

1. Conectarse a internet desde las salas del edificio para atender los requerimientos.
2. Conectarse desde los módems de internet portátil que tiene la compañía.
3. Trabajar desde la casa.

2.3. *Plan de recuperación ante pérdida de la información por (Robo, ciber ataque, daño en máquinas, etc.)*

Ante una incidencia presentada a nivel individual o masivo por los motivos mencionados, se tiene el siguiente protocolo de recuperación de información, debido a que la documentación de la empresa se aloja en la nube de Office 365, en la aplicación de SharePoint e integración con OneDrive.

Microsoft Office 365 garantiza que los datos de SharePoint Online no se pierdan por ningún motivo. Internamente, administran las copias de seguridad por su cuenta, pero no proporcionan ninguna interfaz para acceder o restaurar esas copias de seguridad.

Las copias de seguridad de la colección de sitios se realizan cada 12 horas y se mantienen durante 14 días. Las opciones disponibles para recuperar los datos ante una pérdida accidental o voluntaria son los siguientes:

1. Restaurar documentos desde la papelera de reciclaje
2. Restaurar la documentación desde el historial de versiones.
3. Crear una solicitud de soporte de Office 365 (vea: Opciones de restauración en SharePoint Online)

3.3.1 Desde papelera de reciclaje

Si requiere recuperar un archivo o carpeta eliminada, la cual le haya realizado algún cambio no deseado, puede realizar este procedimiento.

ACTIVIDAD	RESPONSABLE
Acceder al sitio en donde se encontraba la información eliminada	Empleado o contratista
En la parte izquierda encontrará un enlace a la Papelera de reciclaje	Empleado o contratista
Una vez acceda a ella, encontrará en la parte derecha una lista de los archivos y carpetas eliminados. Ubique el que está buscando.	Empleado o contratista
Realice un clic derecho sobre el archivo o carpeta y de clic en restaurar.	Empleado o contratista
Verifique que haya quedado restaurado correctamente	Empleado o contratista


	PLAN DE CONTINUIDAD DEL NEGOCIO	Código: DOC.GE.08
		Actualización: 11 DIC 2019
		Versión: 02
		Página 3 de 7

Gráfico 2

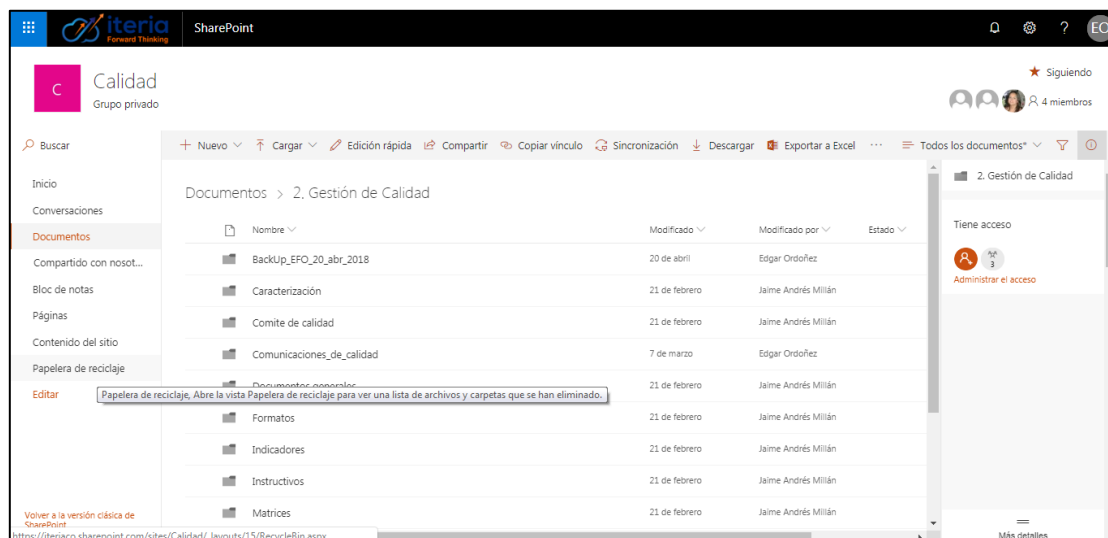
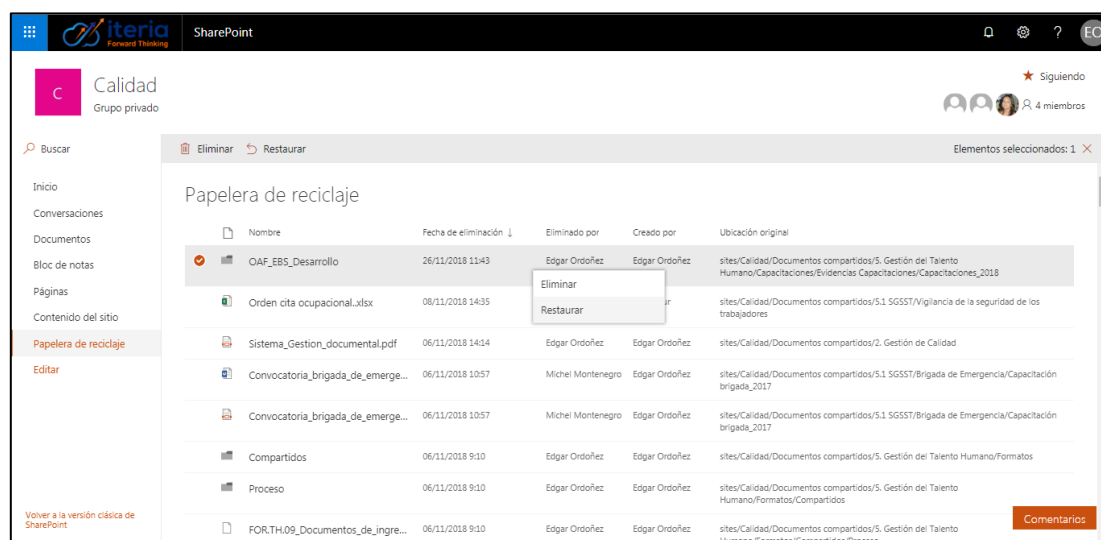


Gráfico 3



3.3.2 Desde historial de versiones

Si requiere restablecer la versión de un archivo, no de una carpeta, a la cual le haya realizado algún cambio no deseado, puede realizar este procedimiento.

ACTIVIDAD	RESPONSABLE
Abrir la aplicación de SharePoint y ubicarse sobre el archivo. Ver gráfico 4.	Empleado o contratista
Hacer clic derecho sobre el archivo y dar clic en historial de versiones	Empleado o contratista
Ubicar la fecha de restauración deseada, darle clic y restaurar	Empleado o contratista


	PLAN DE CONTINUIDAD DEL NEGOCIO	Código: DOC.GE.08
		Actualización: 11 DIC 2019
		Versión: 02
		Página 4 de 7

Gráfico 4

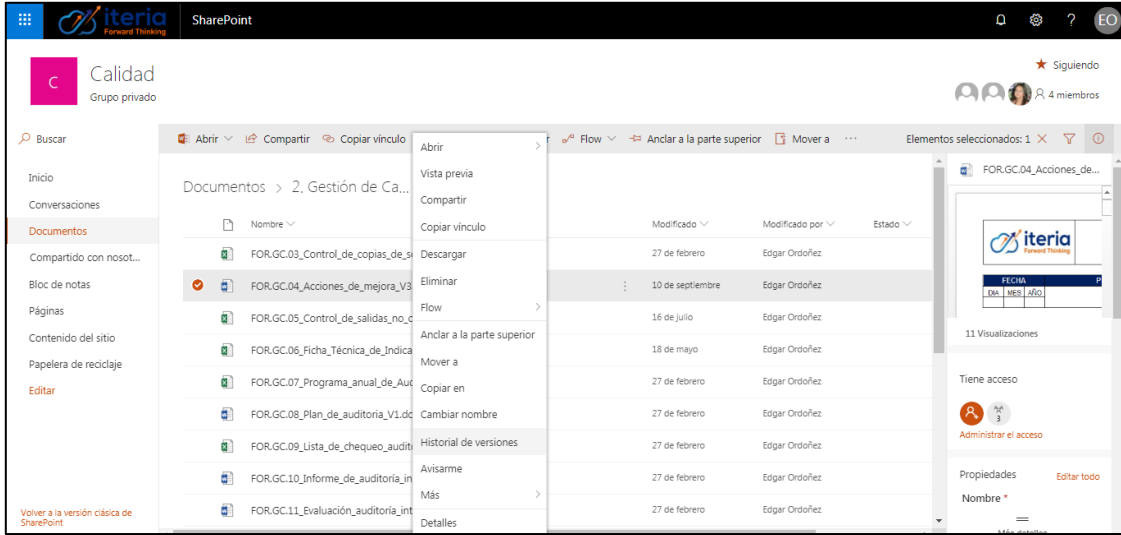
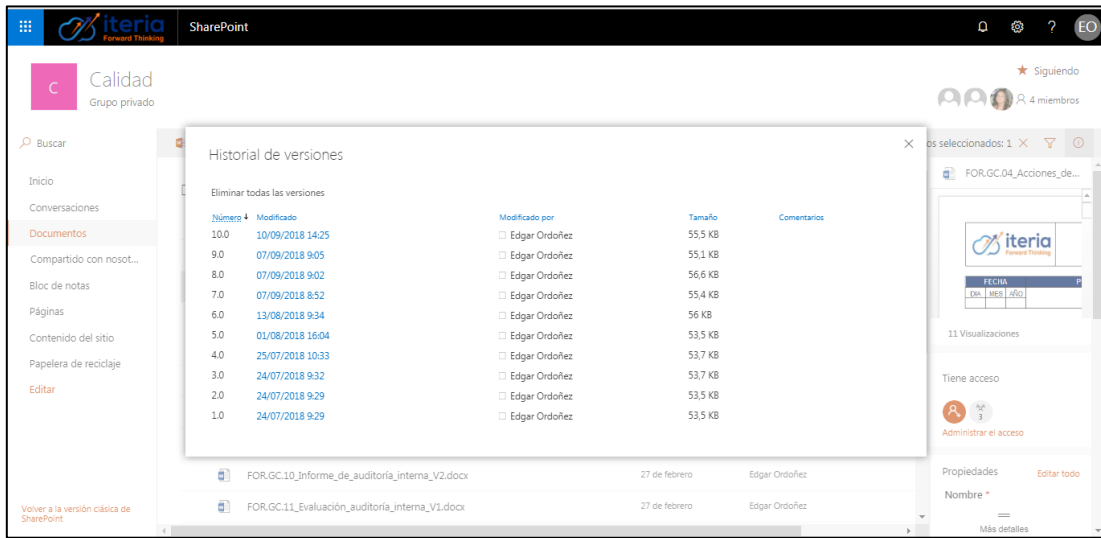



Gráfico 5



3.3.3 Soporte de Office 365

ACTIVIDAD	RESPONSABLE
<p>Cuando detecte una pérdida de información por alguna circunstancia y que deba recuperar, debido a que, en una restauración de la información, los archivos de las carpetas a realizarles el procedimiento también se actualizarán a la fecha requerida de recuperación, se debe realizar una copia de seguridad en su PC de la carpeta a restaurar, para posteriormente actualizar los archivos con los cambios más recientes.</p>	<p>Empleado o contratista</p>

	PLAN DE CONTINUIDAD DEL NEGOCIO	Código: DOC.GE.08
		Actualización: 11 DIC 2019
		Versión: 02
		Página 5 de 7

ACTIVIDAD	RESPONSABLE
Informar al director administrativo y financiero que requiere realizar la operación, indicándole la ubicación de la carpeta o archivos y la fecha de copia de seguridad requerida. Tenga en cuenta las observaciones.	Empleado o contratista
Crear un ticket de soporte a Office 365 y especificar el tiempo de copia de seguridad más antiguo, el tiempo de copia de seguridad más reciente y el tiempo de copia de seguridad óptimo.	Director administrativo y financiero
Una vez realizada la restauración, actualice los documentos que se vieron afectados, reemplazándolos con los archivos que almacenó en su pc.	Empleado o contratista


Recomendaciones a tener en cuenta para recuperación desde Soporte de Office 365

1. Digamos que su colección de sitios fue un desastre durante el día el martes. Puede indicar la primera hora de la copia de seguridad como lunes del cierre de operaciones (por ejemplo, 6 PM), la última hora de la copia de seguridad abierta el martes (por ejemplo, 6 AM) y la hora de copia de seguridad óptima como el martes a las 4 AM. El equipo de soporte le proporcionará la mejor copia de seguridad basada en esta información.
2. Debe tener al menos 12 horas entre los tiempos más antiguos y recientes. La restauración se realiza a una colección de sitios.
3. Si sabe que va a restaurar sobre una colección de sitios existente, puede continuar y bloquear la colección de sitios para que los usuarios no realicen cambios que se sobrescriban.
4. Se reemplazará toda la colección de sitios y se perderán todos los cambios realizados después del tiempo de respaldo (se debe volver a realizar después de la restauración).
5. Una vez que se solicita una restauración, puede tomar 2 o más días para que se realice la restauración. Esto se realiza en función del proceso de triage del soporte de Office 365 y la prioridad percibida de la solicitud. La licencia de inquilino o el número total de usuarios para el inquilino no cambia la prioridad.

4. PLAN DE CONTINUIDAD DE NEGOCIO

4.1 Plan de contingencia ante cortes de energía

Todos los computadores de las oficinas ubicadas en el edificio santa Mónica central, se encuentran conectados a las UPS ubicadas en las oficinas correspondientes, lo que nos permite continuar trabajando normalmente hasta 25 minutos, mientras se restablece el servicio de energía. A cada UPS se le realiza mantenimiento anual, de acuerdo al cronograma de mantenimiento. Si el servicio de energía no se recupera antes que se descarguen las UPS, se debe informar al personal que se traslade a sus casas para trabajar de forma remota.

	PLAN DE CONTINUIDAD DEL NEGOCIO	Código: DOC.GE.08
		Actualización: 11 DIC 2019
		Versión: 02
		Página 6 de 7

4.2 Plan de contingencia frente a desastres naturales e incendios.

En caso de siniestro por desastre natural o incendios, Iteria hará uso de la póliza de seguro multirriesgo que además incluye la siguiente cobertura:

Responsabilidad civil extracontractual:

- Responsabilidad civil, operaciones temporales en el exterior.
- Responsabilidad civil, predios, labores y operaciones,
- Responsabilidad civil gastos médicos de urgencias,
- Responsabilidad civil empleador
- Transporte vehículos propios/terceros no formales
- Responsabilidad civil gastos de defensa
- Responsabilidad civil por daños a terceros

Daños materiales:

- Daños materiales edificio
- Daños materiales maquinaria y equipo
- Daños materiales contenidos
- Daños materiales equipo s de computo
- Terremoto edificio
- Terremoto maquinaria y equipo
- AMIT Y HMAACC edificio
- AMIT Y HMAACC maquinaria y equipo
- AMIT Y HMAACC Contenidos
- Daño interno equipos de cómputo y procesamiento
- Daño interno maquinaria


Definiciones:

- AMIT (Actos malintencionados de terceros)
- HMAACC (Huelga, Motín, Asonada, Conmoción civil)

5 DOCUMENTOS RELACIONADOS

- Microsoft Online 365 SLA Nov 2018.
- DOC.GE.13 política de seguridad de la información.
- DOC.GE.15 Gestión de usuarios en sistemas e información.

Elaborador por: Coordinación de Calidad	Revisado por: Representante por la Dirección	Aprobador por: Director Administrativo
---	---	--

	PLAN DE CONTINUIDAD DEL NEGOCIO	Código: DOC.GE.08
		Actualización: 11 DIC 2019
		Versión: 02
		Página 7 de 7

CONTROL DE CAMBIOS

Versión	Fecha de actualización	Razón del cambio
01	26 nov. 19	Nuevo documento
02	11 dic 19	Actualización de planes ante desastres: Sabotaje y ciber ataques, pérdida de información, cortes de energía, desastres naturales e incendios.