1. **PROCESO:** Gestión de las Tecnologías de la Información

2. **SUB PROCESO:** N/A.

3. **OBJETIVO:** Mantener la seguridad y continuidad de la información en el Sistema, en caso de contingencia.

4. **ALCANCE:** Inicia con la declaración formal de la situación de Crisis y finaliza con la verificación de las funciones de Monitoreo.

5. **DISPOSICIONES GENERALES:**

El plan de contingencia está encaminado a mantener la operatividad de USPEC en el caso que se presente una afectación considerable en la disponibilidad de un activo de información crítico, ya sea por una falla en el activo mismo, o por algo que suceda en su entorno, que lo impacte.

En USPEC, el plan de contingencia para un activo de información en particular estará basado principalmente en la redundancia de componentes, el respaldo de la información, el uso de virtualización y en estrategias de recuperación manual de los sistemas; dependerá de la prioridad y nivel de continuidad que establezcan los valores dados al RTO y RPO para ese activo.

La prioridad y continuidad de los activos de información de la Entidad será consignado en el A3-FO-30 Formato de Análisis de Impacto.

Durante la ejecución de un plan de contingencia se deben conservar los controles de seguridad suficientes para mantener los niveles de protección de confidencialidad, integridad y disponibilidad de la información a los mismos niveles que se tenían antes de que se presentara la afectación. Para esto se deben tener en cuenta los siguientes aspectos:

- **RPO: Recovery Point Objective (Punto Objetivo de Recuperación)**
  Ante una interrupción, es el tiempo máximo de tolerancia permitido para pérdida de datos antes de generar consecuencias inaceptables para la misión de la Entidad. Esta variable, define el lapso en el cual deben llevarse a cabo las copias de respaldo. El valor se analiza ante el evento potencial de una interrupción, teniendo en cuenta que la operación se reanude con los datos existentes en el momento de la interrupción o podría volver a una posición anterior y reconstruir los datos faltantes.

- **RTO: Recovery Time Objective (Tiempo Objetivo de Recuperación)**
  El tiempo en el que una aplicación o sistema de información debe ser restablecido luego de una interrupción, antes de que genere consecuencias inaceptables para la Misión de la Entidad. Este valor se Define con base en el nivel de dependencia de la Misión de la entidad con respecto a la completitud de los datos, a través del cual se establece el nivel de inversión que se deberá hacer para reducir las pérdidas de datos ante un evento de interrupción.

- **Copias de Respaldo:** Se deben efectuar con base en el documento del SGSI "Política de generación y restauración de copias respaldo".

6. DEFINICIONES:

Activo: Cualquier elemento que tiene valor para la organización y que para gestión de riesgos de seguridad de la información se consideran los siguientes tipos: información, actividades y procesos del negocio, software, hardware, personal, redes, organización y ubicación.

Confidencialidad: Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada [Fuente: ISO 27000].

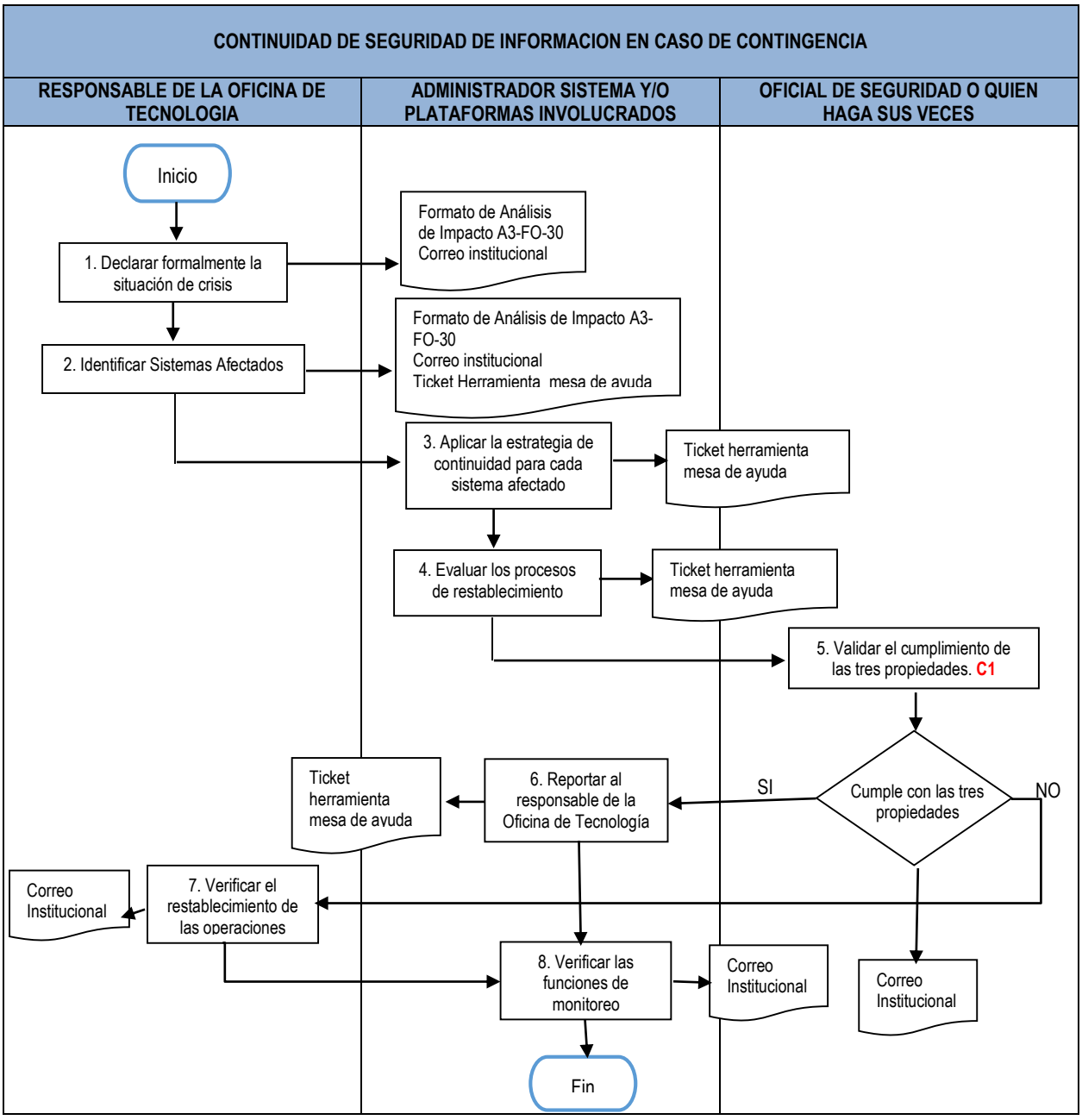
Integridad: Propiedad de precisión y completitud [Fuente: ISO 27000].

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Redundancia: Cuando la opción de las copias de respaldo no satisfaga el RTO y RPO se debe contar con un esquema de redundancia para los componentes de hardware y/o software involucrados.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización) [Fuente: ISO 31000].

7. FLUJOGRAMA:



8. DESCRIPTIVO DEL PROCEDIMIENTO:

N°	Responsable	Registros	D Descripción de la actividad. Cx Punto de Control.	
1	Responsable de la Oficina de Tecnología	Correo institucional Formato de Análisis de Impacto A3-FO-30	**D**	**DECLARAR FORMALMENTE LA SITUACIÓN DE CRISIS:** Se reporta mediante correo electrónico al Jefe de la Oficina de Tecnología la afectación en uno o varios sistemas de información de USPEC. Adicionalmente se deben identificar las áreas afectadas por lo sucedido, teniendo en cuenta el formato A3-FO-30 (formato de Análisis de Impacto) y reportar por correo electrónico a los Directivos, Jefes de Oficina o dueños de proceso.
2	Responsable de la Oficina de Tecnología	Correo institucional Ticket herramienta Mesa de Ayuda A3-FO-30 formato de Análisis de Impacto	**D**	**IDENTIFICAR SISTEMAS AFECTADOS:** Se deben identificar los sistemas afectados, los que deben ser restablecidos y el orden en que se deben restablecer con base en el formato A3-FO-30 (formato de Análisis de Impacto). De igual manera, se debe dar instrucciones vía correo electrónico a los Administradores de Sistema y/o Plataforma involucrados para que inicien con la contingencia y recuperación de estos y crear los casos correspondientes en la mesa de ayuda.
3	Administrador Sistema y/o Plataformas involucrados	Ticket herramienta Mesa de Ayuda	**D**	**APLICAR LA ESTRATEGIA DE CONTINUIDAD PARA CADA SISTEMA AFECTADO:** Se debe ejecutar la contingencia y/o recuperación del sistema afectado y actualizar el estado del caso en la mesa de ayuda.
4	Administrador del Sistema y/o plataformas involucrados	Ticket herramienta Mesa de Ayuda	**D**	**EVALUAR LOS PROCESOS DE RESTABLECIMIENTO:** Se verifica que los procesos de recuperación se están llevando a cabo correctamente y que no afectan otros sistemas, ante cualquier novedad actualizar el caso en la mesa de ayuda.
5	Oficial de Seguridad o quien haga sus veces	Correo Institucional	**D**	**VALIDAR EL CUMPLIMIENTO DE LAS TRES PROPIEDADES:** Se valida que los requerimientos de disponibilidad, integridad y confidencialidad de la información que se cumplían en el sistema antes de la afectación, se

N°	Responsable	Registros	D Descripción de la actividad. Cx Punto de Control.	
			C1	continúan cumpliendo en el momento del restablecimiento del servicio y se notifica por correo al responsable del Sistema y/o Plataformas involucradas. ¿Cumple con las tres propiedades? SI: Continua con la actividad 6 No: Pasa a la actividad 7
6	Responsable del Sistema y/o Plataformas involucradas	Ticket herramienta Mesa de Ayuda	D	**REPORTAR AL RESPONSABLE DE LA OFICINA DE TECNOLOGÍA:** Si los resultados del proceso de recuperación son exitosos se realiza el reporte al responsable de la Oficina de Tecnología, actualizando el estado del ticket en la Mesa de Ayuda. Continúa con la actividad 8.
7	Responsable de la Oficina de Tecnología	Correo Institucional	D	**VERIFICAR EL RESTABLECIMIENTO DE LAS OPERACIONES:** Se realizan pruebas para corroborar que los sistemas afectados se encuentren de nuevo operativos y que se hayan restablecido correctamente todos los servicios asociados. El resultado de esta actividad se informará vía correo electrónico al jefe de la Oficina de Tecnología.
8	Oficial de Seguridad o quien haga sus veces	Correo Institucional	D	**VERIFICAR LAS FUNCIONES DE MONITOREO:** Se verifica que las funciones de monitoreo establecidas dentro de los requerimientos de disponibilidad, integridad y confidencialidad de los activos de información involucrados, se conserven como estaban definidas entes de la afectación. El resultado de esta actividad se informará vía correo electrónico al jefe de la Oficina de Tecnología. Finaliza el procedimiento.

9. PUNTOS DE CONTROL:

Punto de Control	Responsable	Registro
C1: Validar el cumplimiento de las propiedades (confidencialidad, integridad y disponibilidad) con base en lo establecido en el SGSI. En caso que no se cumplan debe reportarse utilizando el procedimiento de Gestión de Incidentes	Oficial de Seguridad o quien haga sus veces	Ticket herramienta Mesa de Ayuda

RESUMEN DE CAMBIOS:

Versión	Fecha	Numerales	Descripción de la modificación
01	24/01/2017	Todos	Se crea el documento

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma: Original firmado	Firma: Original firmado	Firma: Original firmado
Nombre: Alvaro Camargo Barbosa	Nombre: Liliana Cediel Bolaños	Nombre: María Cristina Palau Salazar
Cargo: Analista de Sistemas	Cargo: Coordinadora Grupo Comunicaciones	Cargo: Directora General
Dependencia: Oficina de Tecnologia	Dependencia: Oficina de Tecnologia	Dependencia: Dirección General
	Firma: Original firmado	
	Fernando Vargas	
	Técnico Operativo	
	Dependencia: Oficina de Tecnologia	
	Firma: Original firmado	
	Mayra Alexandra Agudelo	
	Profesional Especializado	
	Dependencia: Oficina de Tecnologia	