FUNDACIÓN SALUD Y NUTRICIÓN	**PLAN DE SEGURIDAD EN LA INFORMACIÓN Y CONTINUIDAD OPERATIVA**	Tipo: Formato
		Versión: 1
		Fecha: 01/09/2020

1. IDENTIFICACIÓN DE LAS FUENTES DE AMENAZA y EVALUACIÓN

Definiciones	
Plan de seguridad:	Son todas aquellas actividades encaminadas a propender por el resguardo y la seguridad de la información, aunque se presente una fuente de amenaza que afecte a la misma.
Tipo:	Se refiere al tipo de peligros que pueden ocasionar la perdida o daños en la informción
Fuente:	Situación o acto con potencial de causar daño en los equipos o en la información
Consecuencia:	Posibles situaciones o resultados que se presentarían en caso de materializarse la situación.
Áreas de mayor riesgo:	Se refiere a los lugares de trabajo común en donde se desarrollan las actividades de la organización: la sede administrativa, los lugares de operación y los lugares de trabajo remoto que principalmente se refiere a los sitios donde se realiza el teletrabajo.
Escenario de continuidad:	Específica de manera global, la acción a proceder, en caso de que se presente la situación
Actividad de continuidad:	Acción a realizar
Responsables:	Persona o personas encargadas de la acción

Descripción de la actividad			
N°	**Tipo**	**Actividad**	**Enlace / Evidencia**
1	**Inicio**	**Identificación de las fuentes de peligro** Determinar cuál de las fuentes de peligro podrían materializarse durante el desarrollo de las acciones de la organización. Escoja en la lista que aparece en cada casilla, las que considere. En caso de que identifica una fuente de peligro que no está enlistada, seleccionar la opción "otra" y especificar en la siguiente columna a cuál se refiere.	Plan
2	**O**	**Identificación de los riesgos desde los procesos** Describa las posibles consecuencias que ocasionaría la materialización de la situación determinada.	Plan
3	**O**	**Determinación del nivel de probabilidad** Determine el riesgo en que se encuentra cada una de estas áreas de trabajo, evaluando en casa uno, del 1 al 3, el nivel de riesgo en que se encuentra, teniendo en cuenta que: 1 (Bajo) La situación nunca ha ocurrido, o solo ha ocurrido una vez en los últimos dos años. 2 (Medio) La situación a ocurrido entre tres a cinco veces en los últimos dos años 3 (Alto) La situación a ocurrido más de seis veces en los últimos dos años	Plan
4	**O**	**Evaluación del riesgo** De acuerdo al resultado anterior se determinará en promedio el nivel de riesgo de cada fuente.	Plan
6	**O**	**Establecer el tratamiento y contingencia** Se especificarán acciones de contingencia para todas las fuentes que tengan un nivel de riesgo mayor a 1.5, y se especificará la persona responsable de ejecutar esta acción.	Plan

	PLAN DE SEGURIDAD EN LA INFORMACIÓN Y CONTINUIDAD OPERATIVA	Tipo: Formato
		Versión: 1
		Fecha: 01/09/2020

Situaciones que ponen en peligro la seguridad de la información	Evaluación						Medidas		
Tipo	Fuente	Consecuencia	Areas en mayor riesgo			Zona de riesgo	Escenario de continuidad	Actividad de continuidad	Responsable
			Adminis.	Sedes	Remotas				
Ambiental	Contaminación	Degradación de equipos y materiales impresos	2	2	1	1,7	Respaldo digital de información	Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
							Subcontratación	Contratación de servicios técnicos para mantenimiento de equipos de computo	Gerente administrativa y financiera
	Incendio forestal	Perdida total o parcial de equipos e información	1	3	1	1,7	Respaldo digital de información	1. Realizar copia digital mensualmente de la información fisica que se tenga 2. Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
	Inundación	Perdida total o parcial de equipos e información	1	3	1	1,7	Respaldo digital de información	1. Realizar copia digital mensualmente de la información fisica que se tenga 2. Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
	Terremoto	Perdida total o parcial de equipos e información	1	1	1	1,0	Respaldo digital de información	1. Realizar copia digital mensualmente de la información fisica que se tenga 2. Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
	Tsunami	Perdida total de equipos e información	1	1	1	1,0	Respaldo digital de información	1. Realizar copia digital mensualmente de la información fisica que se tenga 2. Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
Condiciones de seguridad pública	Ciber terrorismo	Fuga de información Perdida de datos	1	1	1	1,0	Respaldo digital de información	1. Realizar copia digital mensualmente de la información fisica que se tenga 2. Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
	Protestas	Retraso en la recolección, resguardo y entrega de información	3	2	1	2,0	Centro de operación alterno	1. Se realizará traslado temporal a unidades de servicio (sedes) o en trabajo remoto, cuando afecte la sede administrativa 2. Se suspenderá las actividades en la sede y se trasladara a trabajo remoto	Gerente Líder de talento humano
	Robo de equipos	Perdida total o parcial de equipos e información	1	2	2	1,7	Respaldo digital de información	Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
	Vandalismo	Perdida total o parcial de equipos e información	1	2	2	1,7	Centro de operación alterno	1. Se realizará traslado temporal a unidades de servicio (sedes) o en trabajo remoto, cuando se presente en la sede administrativa 2. Se realizará acompañamiento del profesional en caso que el daño se realice en el lugar del trabajo remoto	Gerente Líder de talento humano
							Respaldo digital de información	Realizar back up de toda la información digital que se tenga y mantener en archivo digital compartido	Todo el personal
Condiciones de seguridad locativas	Daño en infraestructura física	Perdida parcial de equipos e información	2	1	2	1,7	Centro de operación alterno	1. Se realizará traslado temporal a unidades de servicio (sedes) o en trabajo remoto, cuando se presente en la sede administrativa 2. Se realizará acompañamiento del profesional en caso que el daño se realice en el lugar del trabajo remoto	Gerente Líder de talento humano
							Traslado de personal	1. Se trasladará el personal a sede temporal si es de tipo operativo 2. Se realizará trabajo remoto en caso que sea de tipo administrativo	Gerente Coodinador
	Falla de suministro de agua	Perdida parcial de equipos e información	1	1	1	1,0	Traslado de personal	1. Se trasladará el personal a sede temporal si es de tipo operativo 2. Se realizará trabajo remoto en caso que sea de tipo administrativo	Gerente Coodinador
	Falla de suministro de energía	Perdida parcial de equipos e información	2	2	2	2,0	Centro de operación alterno	1. Se realizará traslado temporal a unidades de servicio (sedes) o en trabajo remoto, cuando se presente en la sede administrativa	Gerente Líder de talento humano
							Traslado de personal	1. Se trasladará el personal a sede temporal si es de tipo operativo, o a otro lugar de trabajo remoto consertado	Coodinador
	Incendio	Perdida total o parcial de equipos e información	2	2	2	2,0	Centro de operación alterno	1. Se realizará traslado temporal a unidades de servicio (sedes) o en trabajo remoto, cuando se presente en la sede administrativa	Gerente Líder de talento humano
							Traslado de personal	1. Se trasladará el personal a sede temporal si es de tipo operativo, o a otro lugar de trabajo remoto consertado	Coodinador
Psicosocial	Indisponibilidad del personal	Perdida o daños en la información	1	2	2	1,7	Entrenamiento cruzado	Mantener entrenamiento del personal sobre el manejo y ubicación de la información	Gerente Líder de talento humano
	Muerte de personal	Perdida de información	1	1	2	1,3	Entrenamiento cruzado	Mantener entrenamiento del personal sobre el manejo y ubicación de la información	Gerente Líder de talento humano
	Código malicioso (Malware)	Perdida o daños en la información	2	1	3	2,0	Personal de respaldo	1. Solicitar a ingenieros internos revisión de equipos y manejo de la situación 2. Las personas en trabajo remoto deben disponer de sus propios equipos y solicitar revisión con el personal en caso de codigos maliciosos	Gerencia Asistente administrativa

Suministros y equipos	Daño y/o perdida de información	Incumplimiento de servicios	2	2	2	2,0	Subcontratación	Contratación de servicios técnicos de equipos de computo	Gerente administrativa y financiera
	Falla/degradación equipo informático	Perdida total o parcial de equipos e información	2	2	2	2,0	Subcontratación	Contratación de servicios técnicos de equipos de computo	Gerente administrativa y financiera
	Indisponibilidad de producto	Retraso en el cumplimiento del servicio	1	1	1	1,0	Subcontratación	Contratación de servicios técnicos de equipos de computo	Gerente administrativa y financiera

FUNDACIÓN SALUD Y NUTRICIÓN	**CONTROL DE CAMBIOS**	Tipo: Formato Versión: 1 Fecha: 01/09/2020

VERSIÓN	FECHA	REALIZÓ	REVISÓ	APROBÓ	DESCRIPCION DEL CAMBIO
1	1/09/2020	Sara Gómez	Sara Gómez Diaz	Rosaura Bautista C.	Creación del plan