FONPRECON Pensiones y Cesantías	MAPA DE RIESGOS	CODIGO: MAP-SGSI-001
	SEGURIDAD DE LA INFORMACIÓN – SEGURIDAD DIGITAL	VERSIÓN: 1

PORTADA

A) HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN DE LA MODIFICACIÓN
1	22/07/2020	Se crea el mapa de riesgo de Seguridad de la Información – Seguridad Digital contiene 14 riesgos de acuerdo a la Norma Técnica Colombiana NTC-ISO-IEC 27001 y la guía No. 4 del DAFP

B) REVISIONES Y APROBACIONES DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Dr. Luis Enrique Cortés Callejas	Nombre: Dra. Carolina Tobar Sierra	Nombre: Dr. Álvaro Francisco Ramírez Rivera
Cargo: Profesional Especializado Unidad de Riesgo Operativo	Cargo: Jefe Oficina Asesora de Planeación y Sistemas (E)	Cargo: Directora General
Fecha 14/07/2020	Fecha: 21/07/2020	Fecha: 22/07/2020

REVISÓ	REVISÓ
Nombre: Dr. Oscar Alexander Herrera	Nombre: Ing. Jesús Goyes Alvarado
Cargo: Gerente de Calidad	Cargo: Contratista Grupo Tecnología
Fecha: 16/07/2020	Fecha 22/07/2020

FONPRECON Pensiones y Cesantías	MAPA DE RIESGOS	CODIGO: MAP-SGSI-001
	SEGURIDAD DE LA INFORMACIÓN – SEGURIDAD DIGITAL	VERSIÓN: 1

C) LISTA DE DISTRIBUCIÓN

1	Luz Stella Restrepo Henao – Subdirectora Administrativa y Financiera
2	Dr. Paulo Emilio Morillo Guerrero – Jefe Oficina Control Interno
3	Dra. Lydia Edith Rivas Niño – Jefe Oficina Asesora de Jurídica
4	Dr. Armando Ricardo Delgado Suárez – Jefe Oficina Asesora de Planeación y Sistemas
5	Dra. Vilma Leonor García Pabón – Subdirectora de Prestaciones Económicas
4	Dra. Rosa Mary Hernández González – Coordinadora Grupo de Coactivo
5	Dra. Mónica María Garzón González – Coordinadora Grupo Afiliaciones, Aportes e HL
6	Dra. Martha Fabiola López Jiménez – Coordinadora Tesorería
7	Dra. Mary Sandra Arizala Arévalo – Coordinadora de Contabilidad
8	Dra. Piedad Restrepo Jaramillo – Coordinadora Archivo y Correspondencia
7	Dr. Germán Armando correa Amado – Coordinador Presupuesto – Bienes y Servicios
8	Dr. Mario Alberto Cabrera Rico – Coordinador Almacén
9	Dr. Jairo Vargas Rodríguez – Coordinador Talento Humano
9	Dr. Andrés Felipe López González – Coordinador de Jurídica

FONPRECON Pensiones y Cesantías	MAPA DE RIESGOS SEGURIDAD DE LA INFORMACIÓN -SEGURIDAD DIGITAL Norma Tecnica Colombiana NTC-ISO-IEC 27001	CODIGO: MAP-SGSI-001 VERSIÓN 1 Fecha de aprobación 22/07/2020

Nro.	ACTIVOS	RIESGO	DESCRIPCIÓN RIESGO	AMENAZA	TIPO	CAUSA / VULNERABILIDAD	CONSECUENCIA	RIESGO INICIAL O INHERENTE		
								CALIFICACIÓN		EVALUACIÓN
								PROBABILIDAD	IMPACTO	
1	RECURSO HUMANO	Pérdida de Confidencialidad	Practicas inadecuadas en seguridad de la información por parte los funcionarios públicos de Fonprecon	Usuarios mal intencionados o sin conocimientos en seguridad de la información.	Seguridad de Información	1. Falta de revisiones periódicas a la política general y/o a políticas específicas de seguridad de la información. 2. Servidores con privilegios inadecuados de acceso a la información, e inadecuado uso de la información.	. Desactualización de políticas de seguridad de la información . Incumplimiento de políticas de seguridad de la información . Pérdida Imagen institucional . Sanciones disciplinarias o penales	Improbable	Moderado	Moderado
2	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Integridad	Daño de información o en las instalaciones de procesamiento de datos (Datacenter)	Incendio, inundación, polvo, funcionarios con acceso a Datacenter, proveedores tecnológicos, códigos maliciosos (Spyware, Troyanos, Virus, Gusanos) Información inexacta o adulterada	Seguridad de Información	1. Ausencia de planes de emergencia y pruebas al mismo. 2. Ausencia de redes contra incendio. 3. Falta de controles de acceso físico o deficiencia de los mismos. 4. Privilegios inadecuados de acceso para modificar información producida en los diferentes procesos.	.Interrupción completa de los servicios ofrecidos por Fonprecon . Información inexacta .Pérdidas económicas .Pérdida imagen institucional .Sanciones disciplinarias y penales	Improbable	Mayor	Alto
3	HARDWARE SOFTWARE Y SERVICIOS	Perdida de Integridad	Instalación y uso de software con vulnerabilidades conocidas en los sistemas operativos de los equipos de cómputo y servidores	Usuarios mal intencionados, códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), software con vulnerabilidades	Seguridad de Información	1. Ausencia de políticas y controles restrictivos para la instalación de software no autorizado 2. Uso e instalación de software con vulnerabilidades 3. Perfiles y privilegios no asignados	Interrupción de las operaciones y/o afectación en la prestación del servicio	Probable	Mayor	Extremo
4	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Confidencialidad	Infección de equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad, dispositivos móviles) ocasionado por la pérdida de la confidencialidad.	Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), usuarios sin conocimiento de las políticas de seguridad de la información Servidores públicos que utilizan indebidamente las redes informáticas	Seguridad de Información	1. Base de datos de antivirus desactualizada. 2. Uso de medios removibles. 3. Uso de las redes para actividades diferentes a las laborales.	Posibles fallos de seguridad o vulnerabilidades en los equipos informáticos y/o perdida de información sensible y confidencial de Fonprecon	Posible	Moderado	Alto
5	INFORMACIÓN RECURSO HUMANO	Pérdida de Disponibilidad	Pérdida de la información digital dada en custodia al proveedor de Backup's (daño, robo, pérdida)	Proveedores externos, Atacantes, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), servicios de suministro, amenazas naturales (terremotos, incendios, inundaciones, polvo)	Seguridad de Información	1. Manipulación, transporte y almacenamiento inadecuado a las cintas de backups. 2. Ausencia de pruebas regulares a las copias de respaldo.	Perdida de la información y posibles ataques a la integridad de los datos.	Improbable	Menor	Bajo
6	INFORMACIÓN RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Disponibilidad	Pérdida de la información generada por las actividades propias de la gestión del proceso	Administrador de servidores sin conocimiento de las políticas de seguridad de la información, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), Atacantes Utilizacion indebida de dispositivos extraibles para guardar información que reposa en los equipos de cómputo, o carga de energía de dispositivos móviles en las entradas USB.	Seguridad de Información	1. Ausencia de medidas para evitar la pérdida de datos, por ejemplo copias de respaldo. 2. Falta de pruebas regulares a las copias de respaldo. 3. Ausencia de manuales para la administración de las herramientas de aplicaciones. 4. Servideres públicos sin conciencia o conocimiento de los posibles daños o pérdida de información.	Perdida de confidencialidad y disponibilidad de la información para los usuarios internos y externos.	Improbable	Mayor	Alto
7	INFORMACIÓN RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Confidencialidad	Uso inadecuado de los activos de información (tipo servicios, hardware, software, RECURSO HUMANO, información física y digital)	Activos de información, usuarios sin conocimiento de las políticas de seguridad de la información	Seguridad de Información	1. Ausencia de políticas y controles para la gestión adecuada de los activos de información. 2. Falta de sensibilización en el uso adecuado de los activos de información.	Perdida, robo o mala utilización de la información	Posible	Moderado	Alto
8	RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Integridad	Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)	Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), administradores de tecnología sin conocimientos técnicos de seguridad de la información.	Seguridad de Información	1. Vulnerabilidades técnicas sin conocer, uso de software desactualizado 2. Falta de sensibilización del personal sobre ataques cibernéticos	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos Afectación a toda la Entidad	Posible	Moderado	Alto

Nro.	ACTIVOS	RIESGO	DESCRIPCIÓN RIESGO	AMENAZA	TIPO	CAUSA / VULNERABILIDAD	CONSECUENCIA	RIESGO INICIAL O INHERENTE		
								CALIFICACIÓN		EVALUACIÓN
								PROBABILIDAD	IMPACTO	
9	INFORMACIÓN RECURSO HUMANO	Pérdida de Confidencialidad	Gestión y uso inadecuado de las contraseñas	Usuarios sin conocimiento de las políticas de seguridad de la información y sin sensibilización.	Seguridad de Información	1. Ausencia de políticas para la gestión y uso de contraseñas 2. Falta de sensibilización y capacitación en el uso de contraseñas	Incumplimiento de las políticas de seguridad de la información	Probable	Mayor	Extremo
10	RECURSO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Confidencialidad	Acceso no autorizado a las redes de la entidad (interna y externa)	Red sin protección, usuarios mal intencionados, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos)	Seguridad de Información	1. Ausencia de controles que protejan la información transferida y las instalaciones de procesamiento de información de soporte	Perdida de imagen ante los usuarios y perdida de confidencialidad de la información	Improbable	Menor	Bajo
11	RECURSO HUMANO	Pérdida de Confidencialidad	Incumplimiento de las responsabilidades de seguridad de la información asignadas a los funcionarios públicos	Funcionarios públicos, manual de funciones, contratos de prestación de servicios	Seguridad de Información	1. Falta de competencia de las personas para cumplir con las responsabilidades de seguridad de la información asignadas 2. Desconocimiento de las responsabilidades de seguridad de la información 3. Falta de descripción de los roles y responsabilidades asignadas en los documentos de la contratación	Incumplimiento de la política de seguridad de la información y sanción disciplinaria	Posible	Moderado	Alto
12	HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Integridad	Daño en equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad, dispositivos móviles)	Fallas en servicios de suministro (energía, telecomunicaciones, aire acondicionado)	Seguridad de Información	1. Conexión de equipos a corriente no regulada 2. UPS sin revisión o monitoreo 3. Equipos sin protección contra fallas de energía	Afectación a la disponibilidad de los servicios de Fonprecon	Improbable	Mayor	Alto
13	INFORMACIÓN	Pérdida de Disponibilidad	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	Funcionarios con roles de seguridad de la información, códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), Atacantes, Proveedores Críticos	Seguridad de Información	1. Exclusión de la seguridad de la información en la planificación de la continuidad del negocio	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la Entidad	Probable	Catastrófico	Extremo
14	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Disponibilidad	Pérdida de la disponibilidad de las instalaciones de procesamiento de información	Funcionarios y/o Contratistas, Códigos maliciosos (Spyware, Troyanos, Virus, Gusanos), Atacantes, Proveedores Críticos, infraestructura tecnológica, servicios críticos	Seguridad de Información	1. Ausencia de redundancias para los servicios críticos	Perdida de la continuidad de la operación del negocio	Improbable	Mayor	Alto

) DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL

CODIGO: PLN-SGSI-001 VERSIÓN 1 Fecha de aprobación: 22/07/2020

PLAN DE TRATAMIENTO

RIESGO RESIDUAL			OPCION DE TRATAMIENTO	ACCIONES	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO DE EJECUCIÓN		INDICADOR
CALIFICACIÓN		EVALUACIÓN						FECHA INICIO	FECHA FIN	
PROBABILIDAD	IMPACTO									
Improbable	Moderado	Moderado	Reducir el riesgo	Revisiones periódicas y actualización de la política general de seguridad de la información.	1. A.5.1.1 Políticas para la seguridad de la información A. 5.1.2 revisión de la política (NTC ISO-IEC 27001/2013)	Política general de seguridad de la información aprobada por la alta dirección Documento de políticas específicas de seguridad de la información.	Grupo de Tecnología OAPS	30/06/2020	30/12/2020	Acta de revisión y/o actualización (Comité SGSI)
				Revisiones periódicas y actualización del documento de políticas de seguridad de la información.	1.1. A.5.1.1 Políticas para la seguridad de la información (NTC-ISO-IEC 27001/2013)		Alta Dirección	30/06/2020	30/12/2020	Acta de revisión y/o actualización (Comité SGSI)
				Socializar la política general de seguridad de la información aprobada por la alta dirección, por medio de: Correo electrónico, Intranet, Pagina Web, Sensibilizaciones. (Dejar evidencia documentada)	2. El líder del proceso deberá llevar control sobre los permisos de acceso a la información digital o física de cada integrante del equipo de trabajo, contenida en su inventario de activos y que reposa en cada una de las dependencias, para ello deberá informar al área de tecnología sobre los permisos de acceso, efectuar registro de documentación a cargo de cada servidor, con el fin de controlar la confiabilidad de la información, y como evidencia se dejará la respectiva solicitud de privilegios de acceso, así como registro de reparto de expedientes o cualquier documentación que maneje cada área.	Solitud de permisos de acceso a los aplicativos de la entidad Registro de reparto de documentación.	Grupo de Tecnología Líderes de procesos y equipo de trabajo	30/06/2020	30/12/2020	Reuniones, campañas, talleres de socialización (Registro de asistencia)
				Implementar y verificar el cumplimiento de la política general y el documento de las políticas específicas de seguridad de la información.				30/06/2020	30/12/2020	Perdida de disponibilidad, confidencialidad e integridad de la información=Políticas satisfactorias / Políticas medibles * 100
Improbable	Mayor	Alto	Reducir el riesgo	Documentar el plan de recuperación de desastres	1., 2., 3., A.17.1.2 Implementación de la continuidad de la seguridad de la información (NTC-ISO-IEC 27001/2013) 4. los líderes de proceso como su equipo de trabajo deberán cada vez que se entregue información, verificar que sea la misma que reposa en el documento original, para evitar adulteración o inexactitud de la información, como evidencia se dejará en el escrito de entrega, que la información es fiel copia o es sustraída del original que reposa en los archivos.	Sistema de detección y prevención de incendios. Plan de recuperación de desastres para montar servicios en el centro de datos alterno.	SAF Grupo de Tecnología OAPS Líderes de proceso y equipo de trabajo	30/06/2020	30/12/2020	Plan de continuidad de Negocio del sistema CHIP
Probable	Mayor	Extremo	Reducir el riesgo	Establecer e implementar políticas para la gestión de vulnerabilidades técnicas y para la restricción de instalación de software en sistemas operativos	1. A.9.2.3 Gestión de derechos de acceso privilegiado (NTC-ISO-IEC 27001/2013) 2., 3. A.12.6.2 Restricciones sobre la instalación de software (NTC-ISO-IEC 27001/2013)	Perfiles y privilegios de administración asignados para ciertos administradores de las plataformas	Grupo de Tecnología OAPS	30/06/2020	30/12/2020	Reporte Mensual de análisis de vulnerabilidades
				Establecer e implementar procedimiento para la restricción de instalación de software en sistemas operativos				30/06/2020	30/12/2020	Reporte de software instalado en los equipos
				Establecer reglas para el manejo de la gestión de los medios removibles	1. A.12.2.1 Controles contra	Se monitorea con la consola de antivirus ESET version 6		30/06/2020	30/12/2020	Reporte de dispositivos externos escaneados

RIESGO RESIDUAL			OPCION DE TRATAMIENTO	ACCIONES	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO DE EJECUCIÓN		INDICADOR
CALIFICACIÓN		EVALUACIÓN						FECHA INICIO	FECHA FIN	
PROBABILIDAD	IMPACTO									
Posible	Moderado	Alto	Reducir el riesgo	Cumplimiento de las políticas para la protección contra código malicioso en servidores y equipos de cómputo.	malicioso (NTC-ISO-IEC 27001/2013) 2. A.12.2.1 Controles contra códigos maliciosos (NTC-ISO-IEC 27001/2013) 3. Los líderes de proceso deberán tener control sobre la utilización de las redes e internet por parte de su equipo de trabajo, para evitar daños en la información por causa de virus informáticos, para ello, de manera periódica, hará los requerimientos y sensibilización sobre el tema, como evidencia se dejará las comunicaciones respectivas	Al conectar dispositivos USB el antivirus automaticamente realiza un escaneo el cual no se puede cancelar por parte del usuario. Se controlan desde la consola las actualizaciones de las bases de datos de virus.	Grupo de Tecnologia OAPS Líderes de proceso	30/06/2020	30/12/2020	Reporte de código malicioso
Improbable	Menor	Bajo	Asumir el riesgo	Realizar pruebas de restauración de las copias de respaldo de la información, software e imágenes de los sistemas. Validar los requisitos de seguridad en la custodia de cintas al proveedor (Transporte, instalaciones, manipulación, etc)	1. A.12.3.1 Respaldo de información (NTC-ISO-IEC 27001/2013) 2. A.15.1.3 Cadena de suministro de tecnología de información y comunicación (NTC-ISO-IEC 27001/2013)	Vistas de inspección de seguridad al Proveedor que custodia las cintas. Solicitud permanente de cintas dadas a la custodia del Proveedor	Grupo de Tecnologia OAPS	30/08/2020 30/08/2020	30/12/2020 30/12/2020	Especificación de requerimientos de seguridad informática para proveedor de custodia de medios Registro de entrega de medios
Improbable	Mayor	Alto	Reducir el riesgo	Dar cumplimiento con los procesos para la realización de backups a software, imágenes de los sistemas operativos, e información crítica Verificación de las copias de respaldo por medio de pruebas de restauración Campañas de sensibilización	1., 2., 3., A.12.3.1 Respaldo de información (NTC-ISO-IEC 27001/2013) 4. Los líderes de proceso deberán controlar la no utilización por parte del equipo de trabajo, sobre la utilización de las terminales de cómputo, para guardar información en medios extraíbles, o el cargue de bateria de los dispositivos móviles de comunicacion, para evitar daños de la información que reposa en las terminales, para ello impartirá las respectivas instrucciones, y el cumplimiento de las políticas de seguridad de la inforamción, como evidencia se dejarán las respectivas comunicaciones	Implementación de copias de respaldo con frecuencia diarios, semanales y mensuales	Grupo de Tecnologia OAPS Líderes de proceso	30/07/2020	30/12/2020	Verificación del formato GTI02-FOR01 Bitacora plataforma tecnológica
Posible	Moderado	Alto	Reducir el riesgo	Proporcionar un instructivo que brinde la guía para la gestión adecuada de los activos de información	1., 2., A.8.1.1 Inventario de activos (NTC-ISO-IEC 27001/2013) A.8.1.2 Propiedad de los activos (NTC-ISO-IEC 27001/2013) A.8.1.3 Uso aceptable de los activos (NTC-ISO-IEC 27001/2013) Los líderes de proceso y su equipo de trabajo deben tener muy claro cuál es su inventario de activos, y sobre ellos deberá aplicar las políticas de seguridad de la información y el buen uso de las mismas, con el propósito de evitar pérdidas de confidencialidad, para lo cual, los servidores deberán únicamente de la información que requieran para su labor, y como evidencia se tendrá en cuenta el reparto o tareas asignadas	Inventario de hardware y software	Grupo de Tecnologia OAPS Líderes de proceso y equipo de trabajo	30/07/2020	30/12/2020	Formatos de gestión de activos de información diligenciados y actualizados
				Establecer contacto con grupos de interes especializados en seguridad de la información						Soporte de apoyo prestado por grupos de interes (boletin de seguridad)

RIESGO RESIDUAL			OPCION DE TRATAMIENTO	ACCIONES	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO DE EJECUCIÓN		INDICADOR
CALIFICACIÓN		EVALUACIÓN						FECHA INICIO	FECHA FIN	
PROBABILIDAD	IMPACTO									
Posible	Moderado	Alto	Reducir el riesgo	Desarrollar pruebas de vulnerabilidades periódicas	1. A.6.1.4 Contacto con grupos de interés especial (NTC-ISO-IEC 27001/2013) A.12.6.1 Gestión de las vulnerabilidades técnicas (NTC-ISO-IEC 27001/2013) 2. campañas de sensibilización constante sobre ataques cibernéticos, con el fin de tomar las medias por parte de los servidores sobre el uso adecuado de correos y redes de la entidad, para evitar daños en los sistemas y equipos de cómputo, así como la extracción o modificación de la información, como evidencia se dejarán las actas de capacitación	Cierre de puertos Actualización de software para mitigar riesgos de seguridad Pruebas de vulnerabilidad periódicas	Grupo de Tecnologia Lideres de proceso Oficina Talento Humano	30/03/2020	30/12/2020	Informe de pruebas de vulnerabilidad realizado
				Instalación de nuevas versiones de software						
Probable	Mayor	Extremo	Reducir el riesgo	Dar cumplimiento a las políticas de seguridad de la información relacionadas con el uso adecuado de contraseñas por parte de los usuarios	1. A.9.4.3 Sistema de gestión de contraseñas (NTC-ISO-IEC 27001/2013) 2. Todos los servidores son responsables del uso adecuado y personal de las contraseñas de acceso a la red, con el fin de evitar usos indebidos de la información por parte de personal ajeno, se harán campañas periodicas sobre el uso adecuado de las contraseñas, como evidencia se dejarán las actas o correos institucionales	Politicas de control de contraseñas en el servidor de dominio Configuración en el servidor de dominio para cambio de contraseñas cada 45 dias Se realizan sensibilizaciones por medio de los Tips de seguridad informatica	Grupo de Tecnologia OAPS Líderes de proceso y equipo de trabajo	30/04/2020	30/12/2020	Implementación de politicas para el uso adecuado de contraseñas
				Definir e implementar políticas de asignación de contraseñas temporales seguras cuando se crean usuarios						
				Establecer e implementar política de cambio de contraseña de cuentas de administración genéricas cada vez que expire el tiempo de acceso concedido a un funcionario, exfuncionario, contratista y/o proveedor.						
				Implementar sistemas de gestión de contraseñas que aseguren la calidad de las mismas						
				Inclusión en el plan de sensibilización y capacitación tema de uso adecuado de contraseñas.						
Improbable	Menor	Bajo	Asumir el riesgo	A nivel de Switch se deshabilitan los puertos que no estan en uso	1.A.13.1.1 Controles de redes (NTC-ISO-IEC 27001/2013) 1.1. A.13.1.2 Seguridad de los servicios de red (NTC-ISO-IEC 27001/2013) 1.2. A.13.1.3 Separación en las redes (NTC-ISO-IEC 27001/2013) 1.3. Todos los servidores públicos deben propender por el uso adecuado y responsable de la información que reposa en cada proceso tanto física como digital, para evitar pérdidas de la información evitarán el uso de páginas, correos no institucionales	A nivel de Switch se deshabilitan los puertos que no estan en uso	Grupo de Tecnologia OAPS Líderes de proceso y su equipo de trabajo	30/05/2020	30/12/2020	Reporte de puertos deshabilitados
				Autenticación en redes Wi-Fi mediante protocolos seguros (WPA2)		Autenticacion a la Wifi a traves del directorio activo para la red inalambrica corporativa		30/05/2020	30/12/2020	Aplica politicas del directorio Activo Reporte periodico de conectividad
				Uso de protocolos de comunicación seguros (HTTPS)		En la red de invitados se cuenta con seguridad (WPA2)		30/05/2020	30/12/2020	Realizar contrato de certificado SSL para acceso seguro de la pagina del CHIP
				Implementación de servicios y/o equipos que brinden seguridad perimetral				30/05/2020	30/12/2020	Monitoreo de logs
				Separación de la red de la entidad mediante VLANS .				30/05/2020	30/12/2020	Diagrama actualizado de la red por VLAN
Posible	Moderado	Alto	Reducir el riesgo	Dar cumplimiento con el diligenciamiento del acuerdos de confidencialidad para todos los funcionarios públicos de la Entidad	1 , 2 , 3 . A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información (NTC-ISO-IEC 27001/2013)	Cláusula de confidencialidad en los contratos de prestación de servicios	Talento Humano SAF	30/06/2020	30/12/2020	Acuerdos de confidencialidad
				Definir, ejecutar y hacer seguimiento al plan anual de capacitación, educación (formal y no formal) y formación en seguridad de la información				30/06/2020	30/12/2020	Registro de Plan PIC y de capacitaciones
Improbable	Mayor	Alto	Reducir el riesgo	Realizar inspecciones periódicas de los equipos tecnologicos y de respaldo (servidores, UPS, planta eléctrica) para verificar su funcionamiento y ejecutar las correcciones necesarias	1 . 2 . 3 1. A.11.2.2 Servicios de suministro (NTC-ISO-IEC 27001/2013) 1.1. A1.1 . 2.1 . 3.1 . 1.2 La oficina de bienes y servicios, debe contar con un plan de mantenimiento de los equipos tecnológicos, redes eléctricas, y demás elementos necesarios para la preservación y continua prestación del servicio para evitar fallas o daños en la información, como evidencia se dejaran los soportes de los mantenimientos y de la prestación del servicio	Sistema de Alimentación Ininterrumpida (UPS) con autonomia de 1 hora Planta Electrica con autonomia de 10 horas Aire acondicionado	Grupo de Tecnologia Bienes y Servicios	30/06/2020	30/12/2020	Verificación del formato GTI02-FOR01 Bitacora plataforma tecnológica
				Establecer plan de mantenimientos preventivos a los equipos				30/06/2020	30/12/2020	Registro de plan de mantenimientos preventivos

RIESGO RESIDUAL			OPCION DE TRATAMIENTO	ACCIONES	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO DE EJECUCIÓN		INDICADOR
CALIFICACIÓN		EVALUACIÓN						FECHA INICIO	FECHA FIN	
PROBABILIDAD	IMPACTO									
Probable	Catastrófico	Extremo	Reducir el riesgo	Establecer e implementar un plan de continuidad del negocio, en el cual se incluya la continuidad de la seguridad de la información, su verificación y evaluación a la misma	1. A.17.1.1 Planificación de la continuidad de la seguridad de la información (NTC-ISO-IEC 27001/2013) 1.1. A.17.1.2 Implementación de la continuidad de la seguridad de la información (NTC-ISO-IEC 27001/2013) 1.2. A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información (NTC-ISO-IEC 27001/2013)	Backup de las aplicaciones y bases de datos de las apicaciones misionales Plan de Contingencia de la Entidad Plan para la recuperación de desastres Centro de datos ubicado en sitio alterno	Grupo de Tecnologia OAPS SAF Alta gerencia	30/08/2020	30/12/2020	Plan de contingencia Plan de continuidad de Negocio del sistema CHIP
Improbable	Mayor	Alto	Reducir el riesgo	Establecer y poner a prueba sistemas de redundancia suficiente para los servicios y arquitectura critica usados para el procesamiento de información	1. A.17.2.1 Disponibilidad de instalaciones de procesamiento de información. (NTC-ISO-IEC 27001/2013)	Correo electrónico manejado en la nube Centro de datos ubicado en sitio alterno	Grupo de Tecnologia OAPS	30/08/2020	30/12/2020	Informe de pruebas realizado