	Mapa de Riesgos de Seguridad de la Información	Documento Controlado Código: DTIC-R-008 Versión: *03* Fecha de Emisión: *24-02-28* Pagina:

Proceso	Dirección de Tecnologías de la Información y las Comunicaciones	Fecha de Actualización	AA	MM	DD
			24	*4*	*26*

Descripción del Riesgo	Activo	Amenaza	Causas y/o Vulnerabilidad	Consecuencias	Riesgo Inherente			Control Existente (Preventivos y Detectivos)	Control		Riesgo Residual			Opción de manejo				Responsable de la acción	Periodo Seguimiento	Fecha						Acción de contingencia ante posible materialización
					Probabilidad	Impacto	Nivel		Responsable de la aplicación	Periodicidad	Probabilidad	Impacto	Nivel	Aceptar el Riesgo	Reducir el Riesgo	Evitar el Riesgo	Compartir el Riesgo			Inicio			Terminación			
																				AA	MM	DD	AA	MM	DD	
Perdida de Disponibilidad de la información digital alojada en Servidores y equipos de EPA por Interrupción en la continuidad de la información, debido a fallas en los equipos , sistemas de información y/o aplicativos.	. Servidores y equipos de EPA . . Sistemas de Información. . Aplicativos	No disponibilidad del servicio	. Falta de mantenimiento en cableados, racks, ups, *equipos* y /o servidores. . Captura incompleta, *fallas y/o* insuficiencia de los datos procesados en los sistemas de información . . Ausencia, deficiencia o mal manejo en los recursos de almacenamiento y procesamiento. . Manejo inadecuado de la información.	. Falta de acceso a la información . Demora, dilatación, interrupción o atrasos en el funcionamiento de la entidad.	Posible	Mayor	Extremo	. Mantenimientos *preventivos a los diferentes dispositivos,* equipos *y/o* servidores; *durante la vigencia del contrato de mantenimiento.* . Contar con Antivirus y firewall para la protección de la información alojada en los servidores *y/o equipos* de la entidad. . *Soporte en los recursos de almacenamiento y procesamiento de la información, por parte de la Dirección TIC. Y socialización en la intraepa, de la guía para realizar las copias de seguridad.* . Liencias al día , *soporte* y respaldo ~~de~~ los sistemas de información.	Dirección TIC	Anual	Improbable	Mayor	Alto		x			Dirección TIC Gestion de Recursos	Anual	*24*	*1*	*1*	*24*	*12*	*31*	. Solicitar de manera inmediata *la garantia a quien aplique; ya sea* al contratista *de mantenimiento, proveedor de equipos y/o soporte de algun Sistema de Información y/o aplicativo; en caso de fallas en los equipos , sistemas de información y/o aplicativos.*
Perdida de Confidencialidad de la Información digital generada por Equipos obsoletos, software y/o aplicaciones desactualizados, debido a falta de presupuesto.	Software y equipos de cómputo en la entidad	. Pérdida de información. . Retraso en los procesos. . Vulnerabilidad a los ciberataques. . Hurto de medios o documentos.	. Falta de presupuesto para el cambio de todos los equipos de la entidad. . Contar con equipos de computo de más de 5 años de antigüedad y adicionalmente software que a pesar de que cuentan con mantenimiento, son obsoletos debido a la tecnología adoptada. . Almacenamiento de medios sin protección.	. Presencia de errores de configuración o vulnerabilidades que afecten la disponibilidad, integridad y confidencialidad de la información. . Demora, dilatación, interrupción o atrasos en la función institucional.	Posible	Mayor	Extremo	. Cumplir con las solicitudes de actualización de equipos recibidas; una vez al año; basandose en las necesidades y el prespuesto. . Realizar un inventario de los equipos y software que hacen parte de la entidad. . Contratar licencia donde incluya el producto y el soporte técnico del mismo.	Dirección TIC	Anual	Improbable	Mayor	Alto		x			Dirección TIC.	Anual	*24*	*1*	*1*	*24*	*12*	*31*	. *Realizar cambio de* equipos *que presentaron fallas y/o actualizar* software y aplicaciones que sufrieron amenza y se usan dentro de la Empresa.
Perdida de Confidencialidad de la información Digital, debido a Virus Informático y/o ataques cibernéticos, por falta de protección en servidores y equipos de EPA.	.Todos los equipos de cómputo y servidores de la empresa. .Sistemas de Información. .Aplicativos.	. Pérdida o daño de información. . Vulnerabilidades en los equipos, daño y extorsión. . Ataque informático para acceder a información reservada o clasificada, y/o para modificar datos. . Cifrado no autorizado de la información por malware o acción mal intencionada.	. No contar con un sistema de Antivirus y firewall de Protección contra ataques cibernéticos. . Uso de software desactualizado o con vulnerabiidades. . Conexiones a redes públicas sin mecanismos de protección. . Ausencia de controles de detección, de prevención, y de recuperación *en los componentes tecnológicos.*	Cese de actividades o retrasos.	Posible	Mayor	Extremo	. Contrato anual de los servicios de antivirus -Firewall. . Actualización periodica del antivirus en los equipos de computo. . Configuración y control del firewall *y Antivirus*. . *Uso de controles, tales como claves de accesos, formatos de solicitudes, políticas de seguridad, parches de seguridad, alertas, etc.*	Dirección TIC	Anual	Improbable	Mayor	Alto		x			Dirección TIC.	Anual	*24*	*1*	*1*	*24*	*12*	*31*	. Revisión y actualización de equipos faltantes con el actual sistema antivirus . Así como también de los software y aplicaciones que se usan dentro de la entidad. . *Realizar bloqueos y restricciones en caso de encontrarse accesos sospechosos o no permitidos.*
Perdida de Confidencialidad de la Información, debido a Accesos no autorizados en áreas que deberian ser restringidas de manera física y virtual ,por falta de contoles adecuados.	Todos los activos de información de la EPA	. Pérdida de información. . vulnerabilidades en los equipos, daño y extorsión. . Daño en componentes tecnológicos. . Modificación indebida de la información. . Uso no autorizado de la información. . Entrega indebida de la información.	. *Falta de controles de acceso físico a los servidores y equipos de la EPA.* . Falta de controles de acceso físico a las edificaciones , recintos, de la EPA. . Insuficiencia o mal funcionamiento de controles de acceso físico y virtual.	. Pérdida o robo de información. . Fraude.	Posible	Mayor	Extremo	. Implementación de una puerta magnética en el datacenter de la DTIC, con acceso mediante huella, tarjeta magnética y clave secreta. . Para el ingreso de personal a la oficina de la Direccion TIC, se cuenta con un dispositivo biometrico de control de acceso. . Controles de acceso, descritos en los líneamientos, dentro de la Política de Seguridad de la Información, de usuarios, restricciones, uso de contraseñas, mantenimiento de equipos, *etc.*	Dirección TIC	Anual	Improbable	Mayor	Alto		x			Dirección TIC.	Anual	*24*	*1*	*1*	*24*	*12*	*31*	. *Realizar una mayor restricción al Datacenter, que cuente con solo el acceso del Administrador.* . *Realizar cambio inmediato de* contraseñas, *siguiendo las recomendaciones de Mintic, en cuanto a nivel de* seguridad *aceptable.* . Llamado de atención al funcionario, que no esta haciendo uso de los lineamientos de la polítca de seguridad y privacidad de la información.

	Mapa de Riesgos de Seguridad de la Información	Documento Controlado
		Código: DTIC-R-008
		Versión: *03*
		Fecha de Emisión: *24-02-28*
		Pagina:

Proceso	Dirección de Tecnologías de la Información y las Comunicaciones	Fecha de Actualización	AA	MM	DD
			24	*4*	*26*

Descripción del Riesgo	Activo	Amenaza	Causas y/o Vulnerabilidad	Consecuencias	Riesgo Inherente			Control Existente (Preventivos y Detectivos)	Control		Riesgo Residual			Opción de manejo				Responsable de la acción	Periodo Seguimiento	Fecha						Acción de contingencia ante posible materialización
					Probabilidad	Impacto	Nivel		Responsable de la aplicación	Periodicidad	Probabilidad	Impacto	Nivel	Aceptar el Riesgo	Reducir el Riesgo	Evitar el Riesgo	Compartir el Riesgo			Inicio			Terminación			
																				AA	MM	DD	AA	MM	DD	
Perdida de Integridad de la Información, generada por funcionarios, contratistas y demás personal de la EPA; que no hacen uso de los lineamientos y mecanismos; establecidos en las políticas de Seguridad de la Información.	. Todos los equipos de cómputo de la EPA . Información de las bases de datos en los servidores y equipos. . Información confidencial y clasificada perteneciente a la Empresa.	. Pérdida de información, vulnerabilidades en los equipos, daño y extorsión. . Errores humanos en el cumplimiento de las diferentes actividades de su cargo.	. *Falta de cultura, conciencia y/o conocimiento de los usuarios internos de EPA en Seguridad de la Información.* . Falta de seguridad de la información y de los equipos. . Ausencia o carencia de personal idóneo, de conocimientos y habilidades en informática.	Fuga de Información . Retraso en las actividades que se ejecutan dentro de las áreas misionales de la Empresa.	Posible	Mayor	Extremo	. Circulares recordando el buen uso de los lineamientos de la política de seguridad de la información, *la existencia del formato de asignación de perfiles de usuario y la realización de copias de seguridad siguiendo el instructivo publicado en la intranet.* . Controles y restricciones mediante el servidor de dominio, asignación de perfiles y registros existentes. . Capacitaciones sobre el uso y funcionamiento de la Intranet y página web.	Dirección TIC	Trimestral	Improbable	Mayor	Alto		x			Dirección TIC.	Anual	*24*	*1*	*1*	*24*	*12*	*31*	. *Utilizar otros medios para lograr el uso de* los principios de seguridad de la información establecidos en la Empresa, protegiendo los activos tecnológicos por medio de una cultura de seguridad de la información. . Capacitar a los funcionarios sobre la seguridad de la información.
Perdida de Disponibilidad, Confidencialidad e Integridad de la Información Digital debido a la incompatibilidad de los sistemas de información; por la gran cantidad de aplicativos en los diferentes procesos.	Información salvaguardada en la entidad.	Ralentización de los procesos, dispersión y desintegración de los datos	Tener sistemas de información y aplicaciones de manera dispersa e independiente.	Retraso en los procesos, dispersión de la información, vulneración de procedimientos, ralentización de las consultas a la información, entre otros.	Posible	Mayor	Extremo	. Sistematización de procesos e integración con los sistemas de información.	Dirección TIC	Anual	Improbable	Mayor	Alto		x			Dirección TIC.	Anual	*24*	*1*	*1*	*24*	*12*	*31*	. *Solicitar la actualización de* la Intranet *con* las funcionalidades necesarias y transversal a toda la entidad. . *Solicitar a los proveedores a quienes aplica* la compatibilidad de los sistemas actuales y/o la creación de los aplicativos requeridos; que cumplan las condiciones necesarias.

Cargo		
	Elaboró (Líder del Proceso, Profesionales Especializados (Directores Técnicos de los laboratorios)	Revisó y aprobó (Director o Subgerente)

Nota:
Probabilidad: se expresa en términos de frecuencia (trabaja con datos históricos) o factibilidad (se trabaja de acuerdo con la experiencia de los responsables).
frecuencia: implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.
factibilidad: implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.
Niveles de aceptación al riesgo: Para riesgo de corrupción es inaceptable.

Indicadores - gestión del riesgo de seguridad digital
Eficacia:
Porcentaje de controles implementados = No. controles implementados x 100
No. controles definidos

Efectividad:
Riesgos materializados de confidencialidad = No. de incidentes que afectaron la confidencialidad de algún activo del proceso
Variación de incidentes de confidencialidad = (No. de incidentes de confidencialidad en el periodo actual - No. de incidentes de confidencialidad en el periodo previo)*100
Incidentes de confidencialidad en el periodo previo
Riesgos materializados de Disponibilidad = No. de incidentes que afectaron la disponibilidad de algún activo del proceso
Variación de incidentes de disponibilidad = (No. de incidentes de disponibilidad en el periodo actual - No. de incidentes de disponibilidad en el periodo previo)*100
Incidentes de disponibilidad en el periodo previo
Riesgos materializados de Integridad = No. de incidentes que afectaron la Integridad de algún activo del proceso
Variación de incidentes de Integridad = (No. de incidentes de Integridad en el periodo actual - No. de incidentes de Integridad en el periodo previo)*100
Incidentes de Integridad en el periodo previo