SECRETARÍA DISTRITAL DE AMBIENTE

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2020

Sistema de Gestión de Seguridad de la Información

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Con el proceso de identificación de los activos de la SDA se logró identificarlos, clasificarlos, analizarlos, priorizarlos y determinar su valor en caso de pérdida de información, y conociendo los posibles riesgos que puedan afectar la seguridad y privacidad de la información de la entidad.

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos). El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad para la vigencia del 2020.

2. DEFINICIONES

Activos de información: Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte. Se pueden clasificar de la siguiente manera:

1. Personas: Incluyendo sus calificaciones, competencias y experiencia.
2. Intangibles: Ideas, conocimiento, conversaciones.
3. Electrónicos: Bases de datos, archivos, registros de auditoria, aplicaciones, herramientas de desarrollo y utilidades.
4. Físicos: Documentos impresos, manuscritos y hardware.
5. Servicios: Servicios computacionales y de comunicaciones.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Falla: Daño o afectación de un dispositivo por un periodo determinado. Las fallas las podemos clasificar dependiendo del tipo de evento que la ocasione en: fallas accidentales, intencionales o naturales.

Información: Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos. Por ejemplo:

1. Una noticia que escuchamos por la radio.
2. Una señal de tráfico que advierte un peligro.
3. Una fórmula que usamos en un problema.

Acción de tratamiento: Actividad planificada, temporal y única, diseñada y ejecutada para eliminar o reducir las causas de los riesgos o disminuir el impacto de una eventual materialización de los mismos.

Control: Actividad de monitoreo ejecutada sistemáticamente y definida en el marco de actividades establecidas en los procesos, definida con el propósito de reducir la probabilidad o el impacto de la materialización de los riesgos, dando seguridad razonable el cumplimiento de los objetivos

Causas: Fallas, debilidades, condiciones, restricciones o circunstancias ciertas o potenciales, que pueden dar lugar al evento, pueden aumentar la exposición al riesgo o potenciar sus consecuencias.

Consecuencias: Efectos directos e indirectos sobre los recursos y objetivos del proceso si el riesgo se materializa.

Evento: Incidente u ocurrencia interna o externa al proceso, que se da en un lugar o espacio de tiempo particular, de forma súbita o accidental y que impacta el cumplimiento de los objetivos de un proceso.

Indicador de riesgo: Es una herramienta de medición que permite monitorear, de manera preventiva, el comportamiento de los riesgos. Indica cambios en el nivel o exposición a los mismos y permite la identificación de tendencias en el comportamiento de los mismos, generando alarmas tempranas que conducen a reforzar o enfocar la gestión para evitar su materialización.

Riesgo: Todo evento de ocurrencia incierta que de materializarse genera un impacto, positivo o negativo, en el logro o cumplimiento de los objetivos de los procesos o proyectos. Se puede medir en términos de la probabilidad de ocurrencia y el impacto de sus consecuencias.

Riesgo de Seguridad de la Información: Evento que afecta o amenaza la confidencialidad, integridad y disponibilidad de la información y puede impactar las funciones el logro de los objetivos organizacionales.

3. OBJETIVOS PLAN DE TRATAMIENTO DE RIESGOS 2020

El objetivo de este documento es Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital que aplican para la SDA y de esta forma alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

OBJETIVOS ESPECÍFICOS DEL PLAN

- Establecer el plan de tratamiento de riesgos
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos
- El análisis de riesgo deberá cubrir la totalidad del alcance establecido del tratamiento en donde se tomará la Matriz de Activos de Información cuyo resultado de Criticidad sea alto.

4. MARCO LEGAL

ITEM	NORMA	DESCRIPCIÓN
1	NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
2	NTC/ ISO/IEC 27002	Se centra en las buenas prácticas para gestión de la seguridad de la información, utilización de la norma para apoyar la implantación del SGSI en cualquier tipo de organización.
3	Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
4	NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices

5. MARCO REFERENCIAL

Se determinan las características o aspectos esenciales del ambiente en el cual la Entidad busca alcanzar sus objetivos. Se pueden considerar los siguientes factores referenciales que se pueden aplicar a la SDA.

- Estructura Organizacional
- Funciones y Responsabilidades
- Políticas, Objetivos y Estrategias implementadas
- Recursos y Conocimientos con que se cuenta (personas, procesos, sistemas, tecnología)
- Relaciones con las partes involucradas
- Cultura Organizacional

Identificar amenazas: Las amenazas pueden ser el resultado de actos deliberados o mal intencionados que afectan los activos de los procesos. Las organizaciones enfrentan numerosas amenazas comunes tales como el potencial de falla de un servidor o la pérdida del fluido eléctrico; pero también enfrentan otras amenazas que son específicas para esta entidad o son únicas consideradas desde el punto de vista de su impacto potencial.

Para la identificación de las amenazas a las que pueden enfrentarse los procesos críticos del negocio se realizaran entrevistas con funcionarios y contratistas, que suministrarán información sobre cuáles son las amenazas con mayor impacto desde la perspectiva de continuidad del servicio o negocio, las que podrían llegar a afectar la continuidad de los procesos y por consiguiente, podrían causar una pérdida financiera o afectación de la imagen para la SDA

Identificar causas o vulnerabilidades: En esta actividad se establece el conjunto de causas de posibles riesgos que posee cada activo crítico, que, en caso de ser explotadas por una o varias amenazas, afectarían la continuidad del proceso. Las vulnerabilidades,

por su parte, son debilidades o ausencia de controles que un activo perteneciente a un proceso pueda tener.

Algunas de las causas de riesgos consideradas dentro de esta metodología son:

1. Ausencia de políticas
2. Configuraciones no seguras
3. Errores de configuración.
4. Errores de mantenimiento.
5. Errores del administrador.
6. Errores en código.
7. Exposición a materiales peligrosos.
8. Fallas de usuarios.
9. Manuales de uso no documentados
10. Medidas de protección de acceso inadecuadas
11. Medidas de protección física inadecuadas
12. Procesos o procedimientos no documentados.
13. Usuario desinformado.
14. Tecnología inadecuada.
15. Debilidad o inexistencia de controles.

Por otra parte, para poder realizar una eficaz labor preventiva en relación a los riesgos de seguridad de la información es fundamental realizar una precisa identificación de todos y cada uno de los riesgos que existen y que en un momento dado pueden afectar la confidencialidad, la integridad y la disponibilidad de los activos de información del SENA. Del análisis de riesgo se pueden obtener las causas que provocan estos riesgos, las causas que los originan, las vulnerabilidades existentes, los controles existentes y su efectividad, el riesgo inherente, y finalmente el riesgo residual, que con base en este último se definen los planes de tratamiento que mitigan estos riesgos, que por sus características sobre pasas el nivel de apetito al riesgo de la Entidad.

La finalidad de esta fase plan de tratamiento en los riesgos es descubrir, reconocer y registrar los posibles riesgos que afecten a la seguridad de la información. Este proceso incluye la identificación de las causas y el origen de los riesgos, los sucesos o situaciones que pueden tener un impacto en los objetivos de la organización.
El procedimiento para la gestión de riesgos contiene el reconocimiento de las causas y la procedencia del riesgo que puedan afectar a los objetivos.

El método de identificación del riesgo se basa en: Evidencias Mesas de trabajo con los líderes de cada activo, listas de verificación y revisiones de datos históricos sobre activos y riesgos.

Los pasos para la evaluación del riesgo serán:

- Identificación de los riesgos
- Amenazas
- Vulnerabilidades
- Análisis del riesgo
- Valoración del riesgo
- Riesgo inherente
- Riesgo residual
- Definición de los planes de tratamiento

6. METODOLOGIA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se

estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
Activos de Información 2020	Aceptación de Activos de Información	Revisión con todos los responsables de la aceptación de la matriz de activos Aprobación final de todas las matrices y consolidación para posterior publicación	Matriz Final de Activos de Información	Líder de Gestión Documental, Líder de Transparencia, Líder de Seguridad de la Información, Líder Datos Abiertos, Líder SIG para Seguridad	X		
	Publicación de Activos de Información	Publicación de la matriz de Activos	Matriz de Activos en el portal de la entidad	Líder Seguridad de la Información, Líder de Gestión Documental Líder de Transparencia Dependencia de comunicaciones y Web Master	X		
	Levantamiento de Activos de Información en el Módulo de Isolucion.	Los enlaces SIG de la entidad ingresen la información al módulo de seguridad de la información en isolucion	Módulo de Seguridad de isolucion con la información de las matrices.	Líderes SIG de cada Área de la entidad	X		
	Revisión y aceptación de los activos de información subidos a la plataforma isolución por parte de seguridad de la información	Revisión y aceptación de los activos	Revisión y aceptación de los activos subidos por parte de los líderes SIG al módulo de seguridad de la información	Líder de Seguridad de la Información	X		
Gestión de Riesgos 2020	Actualización de lineamientos de riesgos 2020	Actualización de la metodología de riesgos asociado a seguridad de la información	Documento de riesgos actualizado	Líder SIG de seguridad de la información, Líder Seguridad de la Información. Líder Riesgo de la SDA	X		

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
	Actualización e Identificación de Riesgos de Seguridad y Privacidad de la Información, y Seguridad Digital a 2020	Documento con la Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital a 2020	Documento con la identificación, Análisis y Evaluación de Riesgos	Enlace SIG de los procesos Líder Seguridad de la Información. Administrador del riesgo de la SDA		X	
	Aceptación de Riesgos Identificados 2020	Documento con la realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Documento Final	Enlace SIG de los procesos Líder Seguridad de la Información. Administrador del riesgo de la SDA		X	
		Aceptación, aprobación Riesgos identificados y planes de tratamiento	Documento oficial de aprobación			X	
	Publicación de Matriz de Riesgos 2020	Publicación Matriz de riesgos	Matriz de riesgos publicada	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de comunicaciones y Web Master		X	
	Seguimiento Fase de Tratamiento 2020	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Documento con el seguimiento	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de comunicaciones y Web Master		X	
	Evaluación de riesgos residuales 2020	Evaluación de riesgos residuales	Documento con la evaluación de los riesgos residuales	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de		X	

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD							
Gestión	**Actividades**	**Meta**	**Verificación**	**Responsables**	**CRONOGRAMA CUATRIMESTRAL**		
				comunicaciones y Web Master			
	Mejoramiento de estado de riesgos de acuerdo con el PHVA	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Documento Final	Líder Seguridad de la Información, Líder de Riesgos de la SDA. Líder de Transparencia. Dependencia de comunicaciones y Web Master		X	

7. DESARROLLO DE LA METODOLOGIA

• **Fase I: Análisis de la información**: En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores de los procesos, se desarrollarán las siguientes actividades: - Aplicar las políticas de tratamiento de riesgos. - Determinar los controles (se desprenden de las medidas) aplicados en la SDA. - Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

• **Fase II: Desarrollo de los proyectos** En esta fase se realizarán las actividades que permitan la estructuración de las medidas. - Determinar el nombre de la medida. - Definir los responsables de cada medida. - Establecer el objetivo de cada medida. - Elaborar la justificación de la medida. - Definir las actividades a realizar para el desarrollo de la medida**.**

• **Fase III: Análisis de los proyectos:** Definición de los controles relacionados con cada medida. - Validar los riesgos mitigados por cada medida. - Análisis de la aplicabilidad de las medidas. - Priorización de las medidas.

• **Fase VI: Definición del organigrama de responsabilidad del tratamiento:** En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida teniendo en cuenta su estructura organizacional para la gestión de riesgos. -

Identificación de las funciones en materia de seguridad de la información. - Definición del grupo de trabajo de gestión de riesgo de la SDA. - Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas a tomar

Fase V: Ciclo de vida del tratamiento de riesgos: Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

8. RECOMENDACIONES

Es importante que se cuente con un equipo de recurso humano adecuado capaz y suficiente en seguridad de la información y seguridad informática para llevar a buen término el cronograma propuesto de la identificación, tratamiento y mitigación de los riesgos para 2020 en la SDA.

Se debe contar con todo el apoyo del SIG referente a Riesgos de la entidad

Debe existir mayor integración entre los oficiales de Seguridad de la Información, Oficial de Cumplimiento (Trasparencia) y Oficial de Datos Personales (Privacidad) y Líder de Riesgos en la SDA

La integración de seguridad de la seguridad de la información debe ser multidisciplinar y recaer en todos los funcionarios y contratistas de la SDA.

ES de suma importancia luego de tener ya definida y publicada la matriz de activos de información de la SDA realizar la Matriz de Riesgos de acuerdo a las ponderaciones obtenidas en la medición de confidencialidad, integridad y disponibilidad de la información.

Luego de subsanar las observaciones pertinentes de la OCI se debe programar la primera auditoria NTC- ISO 27001:2013 para la vigencia 2020