BENEFICENCIA DEL VALLE DEL CAUCA E.I.C.E
Plan de tratamiento de riesgos y de seguridad de la información

Contenido

I. OBJETIVO

Definir la metodología de gestión de riesgos de seguridad y privacidad de la información, a través de la identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y el tratamiento de los riesgos.

II. DEFINICIONES

Amenaza: Circunstancia o evento que puede provocar daños en los sistemas de información produciendo pérdidas tangibles o intangibles.

Confidencialidad: Condición que brinda un nivel de seguridad, el cual asegura que la información sea asequible sólo por las personas autorizadas.

Disponibilidad: Poder acceder de manera oportuna a los datos y servicios en el momento que se requiera.

Integridad: Certeza de que la información y los datos contenidos en el sistema no han sufrido modificaciones sin autorización.

Modelo de Seguridad y Privacidad de la Información (MSPI): Conjunto de lineamientos, políticas, normas y procedimientos que promueven la seguridad y privacidad de la información.

Riesgo: Grado de exposición de un activo en donde un agente de amenaza pueda tomar ventaja de una vulnerabilidad causando impacto a la organización.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Vulnerabilidad: Son Aquellas debilidades que se presentan en los sistemas, lo cual la hace susceptibles de ser afectada, alterada o destruida por alguna circunstancia indeseada afectando su correcto funcionamiento.

III. FASES

Un Plan Estratégico de Seguridad informática está basado en un conjunto de políticas de seguridad elaboradas a partir de una evaluación de los riesgos a los que están expuestos los activos de información, que indicará el nivel de seguridad en el que se encuentre la entidad. Con el fin de identificar, medir, controlar y monitorear los riesgos existentes, se proponen las siguientes fases:

1. Identificación de activos de información

Se identifican los activos más relevantes y con mayor valor para la Beneficencia del Valle con el apoyo del área de sistemas, ponderando su impacto a nivel de confidencialidad, integridad, y disponibilidad. Los activos se agrupan en las siguientes categorías: Datos e Información, Claves Criptográficas, Servicios, Software, Hardware, Redes de Comunicaciones, Soportes de Información, Equipamiento Auxiliar e Instalaciones.

2. Identificación de los riesgos

Se identifican las diferentes amenazas y vulnerabilidades a los que están expuestos los activos de información. Generalmente se distinguen tres tipos de amenazas:

- **Criminalidad:** acciones causadas por la intervención humana, que violan la ley y que son penalizados.

- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, y también aquellos que son causados indirectamente por la intervención humana.

- **Negligencia y decisiones institucionales:** son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema.

Las vulnerabilidades, a su vez, se pueden agrupar en las siguientes categorías: Ambiental, Económica, Social e Institucional.

3. Estimación de la probabilidad

Se estima de acuerdo con la frecuencia de ocurrencia del evento

TABLA DE PROBABILIDAD

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

4. Estimación del impacto

Luego de identificada la probabilidad de ocurrencia, se estima el daño sobre el activo, derivado de la materialización de la amenaza.

TABLA DE IMPACTO

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

5. Estimación del riesgo

Con base en la determinación de la probabilidad y la valoración del impacto, se establecen los niveles de riesgos y las acciones requeridas de acuerdo con el siguiente esquema:

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo baja: asumir el riesgo

M: Zona de riesgo moderada: asumir el riesgo, reducir el riesgo

A: Zona de riesgo alta: reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgo extrema: reducir el riesgo, evitar, compartir o transferir

6. Plan de tratamiento

La formulación de actividades de tratamiento de riesgos de seguridad de la información implica la identificación de los controles existentes y la implementación de nuevos controles, acorde al nivel de riesgo y a la disponibilidad de recursos.

Es importante además definir el tipo de control a implementar:

- **Preventivo:** aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

- **Correctivo:** aquellos que permiten el restablecimiento de la actividad, después de ser identificado un evento no deseable, también la modificación de las acciones que propiciaron su ocurrencia.

- **Detectivo:** aquellos que detectan un evento no deseable cuando se están ejecutando y por tal razón impiden la materialización del riesgo.

PÁRAMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			15
	Existen manuales instructivos o procedimientos para el manejo de la herramienta			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de la ejecución del control y seguimiento es adecuada.			25
	TOTAL			100

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
	CUADRANTES A DISMINUIR EN LA PROBABILIDAD	CUADRANTES A DISMINUIR EN EL IMPACTO
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

7. Mapa de Riesgos

La documentación del registro de los riesgos detectados se realiza utilizando el formato SE-FO-015 Mapa de Riesgos de Informática, disponible en el aplicativo DARUMA de la entidad. Ver Anexo 1

8. Seguimiento y evaluación

Es importante llevar el registro de acciones de seguimiento para cada uno de los controles implementados en el Plan de tratamiento, con el fin de evaluar la eficacia en su implementación, adelantando verificaciones como mínimo una vez al año o cuando se considere necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo anual debe estar a cargo de los responsables de los procesos, la Oficina de Control Interno y la Jefatura de Sistemas, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.

Anexo 1. SE-FO-015 Mapa de Riesgos Informática

BENEFICENCIA DEL VALLE DEL CAUCA E.I.C.E																			
PROCESO DE SEGUIMIENTO Y EVALUACIÓN	FORMATO MAPA DE RIESGOS												CÓDIGO:	SE - FO - 007					
													FECHA DE:	1/06/2018					
													VERSIÓN:	7					
ÁREA: DIRECCION DE CONTROL INTERNO PROCESO: Seguimiento y Evaluación					Actualizó: Director de Control Interno		Fecha: 30/05/2018								Realizo: Gerente General Revisó: Comité de Gerencia		Fecha: 30/05/2018 Fecha: 30/05/2018		
IDENTIFICACIÓN DEL RIESGO					ANÁLISIS DEL RIESGO			MEDIDAS DE MITIGACIÓN					PLAN DE MANEJO						
Riesgo	Proceso Relacionado	Tipo de Riesgo	Factor Generador del Riesgo (Causa)	Consecuencias	Probabilidad	Impacto	Evaluación del Riesgo Inherente	Controles Existentes	Probabilidad	Impacto	Valoración del Riesgo	Opción de Manejo	Acciones Preventivas	Responsable de la acción	Periodo Seguimiento	Fecha de Inicio	Fecha de terminación	Acción de contingencia ante posible materialización
Vulnerabilidad de los sistemas que impide el desarrollo tecnológico de la entidad afectando su competitividad	Asesoría y Apoyo Tecnológico	Operativo	Resistencia a cambios tecnológicos	Pérdida de competitividad	3	3	Alto	Asesor externo en seguridad informática	2	3	Moderado	Asumir el riesgo / Reducir el riesgo	Visitas periódicas de control / monitoreo	Jefe de Informática	Mensual	01/01/20	31/12/20	Equipos y herramientas informáticas de contingencia
Dificultad para satisfacer las necesidades de la entidad en innovación tecnológica en cuanto a recursos humanos, físicos y económicos	Asesoría y Apoyo Tecnológico	Operativo	Capacidad instalada para la innovación tecnológica	Pérdida de competitividad	3	5	Extremo	Plan Estratégico de Tecnología	2	4	Alto	Reducir el riesgo, evitar, compartir o trasnferir	Seguimiento al PETI	Jefe de Informática	Semestral	01/06/20	31/12/20	Ajuste al PETI
Ejecución de procesos manuales para la entrega de información	Asesoría y Apoyo Tecnológico	Operativo	Tecnología utilizada en los procesos de la entidad	Toma de decisiones con base en información no fiable, errada u obsoleta	4	4	Extremo	Plan de actualización de aplicativos de software	2	3	Moderado	Reducir el riesgo, evitar, compartir o trasnferir	Seguimiento al PETI Seguimiento plan de acción	Jefe de Informática	Semestral	01/06/20	31/12/20	Aplicación del Plan de continuidad del negocio
Vulnerabilidad de los datos	Asesoría y Apoyo Tecnológico	Operativo Seguridad Digital	Incumplimiento de la política de seguridad y tratamiento de datos	Afectación a la normatividad	3	4	Extremo	Plan de tratamiento de datos y política informática	2	2	Moderado	Reducir el riesgo / mitigar	Socialización política de tratamiento de datos y Política informática	Jefe de Informática	anual	01/06/20	01/06/20	Aplicación de la normatividad