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.

Beneficencia del Valle del Cauca E.I.C.E
Calle 9 Nº 4-50 Pisos 9 - 12
Edificio Beneficencia del Valle del Cauca
Línea de WhatsApp: 317 427 3896 - Línea fija (602) 8823249 Ext. 3000
sercliente@loteriadelvalle.com - ventanillaunica@loteriadelvalle.com
www.benevalle.gov.co - www.loteriadelvalle.com

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.

- **Sistemas de información y plataforma tecnológica vulnerables, personal sin los conocimientos suficientes o con privilegios superiores a los de sus funcionaes.**

- **Perdida de disponibilidad de los servicios de internet, Sistema de información, servidores, equipos perifericos**

Las vulnerabilidades, a su vez, se pueden agrupar en las siguientes categorías: Ambiental, Económica, tecnológica, fraude, social e institucional.

3. Estimación de la probabilidad

Se estima de acuerdo con la frecuencia de ocurrencia del evento

Tabla Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta minimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

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.

	Afectación económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 11 y 50 SMLMV.	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 51 y 100 SMLMV.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 101 y 500 SMLMV.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 501 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario sostenido a nivel país.

Fuente: Guía para la administración del riesgo versión 5 - DAFP

Beneficencia del Valle del Cauca E.I.C.E
Calle 9 Nº 4-50 Pisos 9 - 12
Edificio Beneficencia del Valle del Cauca
Línea de WhatsApp: 317 427 3896 - Línea fija (602) 8823249 Ext. 3000
sercliente@loteriadelvalle.com - ventanillaunica@loteriadelvalle.com
www.benevalle.gov.co - www.loteriadelvalle.com

5. Tabla Valoración de controles

Tabla Atributos de para el diseño del control

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

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. Va hacia las causas del riesgo, aseguran el resultado final esperado.

- **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. Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.

- **Detectivo:** aquellos que detectan un evento no deseable cuando se están ejecutando y por tal razón impiden la materialización del riesgo. Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.

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 Matriz Mapa de Riesgos Informática

Formato Mapa Riesgos

Proceso: Asesoría y Apoyo Tecnológico

Objetivo: Gestionar la disponibilidad, confiabilidad y la innovación tecnológica de los servicios y recursos de informática en la entidad.

Alcance: Aplica para todas las actividades del proceso

Identificación del riesgo							Análisis del riesgo inherente						Evaluación del riesgo - Valoración de los controles									Evaluación del riesgo - Nivel del riesgo residual						Plan de Acción					
																Atributos																	
Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
1	Económico y Reputacional	Sistemas de información y plataforma tecnológica vulnerables, personal sin los conocimientos suficientes	poco presupuesto asignado al área	Posibilidad de afectación operacional debido a sistemas de información y plataforma tecnológica vulnerables, personal sin los conocimientos suficientes por el poco presupuesto asignado al área	Fallas Tecnológicas	365	Media	60%	El riesgo afecta la imagen de de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	Mayor	80%	Alto	1	Se cuenta con una persona natural o jurídica en seguridad informática el cual permanentemente está realizando validaciones, seguimientos y monitoreando todo el tráfico entrante y saliente de la red, así como la configuración y actualización de las herramientas de seguridad informatica.	Probabilidad	Preventivo	Manual	40%	Documentado	Aleatoria	Con Registro	Baja	36%	Mayor	80%	Alto	Aceptar						
													2	Se han divulgado las políticas de informática con todo el personal de la empresa.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	22%	Mayor	80%	Alto	Aceptar						
													3	Se ha solicitado la asignación de recursos económicos y físicos orientados a seguridad informática	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Muy Baja	13%	Mayor	80%	Alto	Aceptar						
													4																				
													5																				
													6																				
2	Económico y Reputacional	Pérdida de disponibilidad de los servicios de internet, servidores y equipos periféricos	Fallas técnicas en el operador o sabotajes	Posibilidad de afectación de las operaciones de sistemas debido a la pérdida de disponibilidad de los servicios de internet, servidores y equipos periféricos debido a fallas técnicas en el operador o sabotajes	Fallas Tecnológicas	365	Media	60%	El riesgo afecta la imagen de alguna área de la organización	Leve	20%	Moderado	1	Se realiza constante monitoreo a los dispositivos periféricos, servidores y tráfico en la red tanto de entrada como de salida a través de las herramientas tecnológicas con que cuenta la entidad.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro	Baja	36%	Leve	20%	Bajo	Aceptar						
													2	Se cuenta con canal alterno para el acceso a internet	Impacto	Correctivo	Automático	25%	Documentado	Continua	Con Registro	Baja	36%	Leve	15%	Bajo	Aceptar						
													3	Se cuenta con servidores virtuales en ambiente web como contingencia	Impacto	Correctivo	Automático	25%	Documentado	Continua	Con Registro	Baja	36%	Leve	8%	Bajo	Aceptar						