Empresa de Servicios Públicos Domiciliarios de Lebrija E.S.P.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE LEBRIJA E.S.P

LEBRIJA

2022

TABLA DE CONTENIDO

TABLAS

1. INTRODUCCIÓN

La Empresa de Servicios Públicos Domiciliarios de Lebrija, ha establecido una política para el apoyo y compromiso frente a lo relacionado con la Seguridad de la Información, que podemos encontrar en la Resolución 0137 de 2018. Esta política, se basa en una orientación que requiere el desarrollo de una cultura administrativa de carácter preventivo en la empresa, de tal manera, al lograr comprender el concepto de riesgo, así como el contexto, para lograr por medio de acciones que ayuden a reducir la afectación a la entidad, en caso de materialización de estos. Por otro lado, se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que puedan comprometer el cumplimiento de los objetivos establecidos en el entorno digital.

Lo anterior adoptando las buenas prácticas y los diferentes lineamientos el estándar ISO 27001:2013, alineando con ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas

2. ALCANCE

Con ayudad de este documento, se pretende fortalecer la implementación de acciones para el tratamiento de riesgos de seguridad y privacidad de la información de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, enfocados a la seguridad de los sistemas manejados en la entidad frente a ciberamenazas, como un aporte a las acciones que realizará la entidad en torno a la seguridad y privacidad de la información, teniendo en cuenta las capacidades y recursos disponibles, para mejorar la confianza de los usuarios, socios y demás partes interesadas.

3. OBJETIVO

Instaurar un marco de acción para aportar al tratamiento de riesgos de seguridad y privacidad de la información, sobre los activos de tecnologías de información que soportan la prestación de servicios digitales en la entidad, desde un enfoque de la seguridad informática frente a diferentes tipos de ciberamenazas, mediante el cual se definen acciones para aportar al tratamiento de riesgos de seguridad y privacidad.

4. DEFINICIONES

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Análisis de riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que modifica el riesgo. Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud. Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- **Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo.
- **Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

5. CLASIFICACIÓN DE RIESGOS INFORMÁTICOS

A continuación, se establece la clasificación de riesgos y su explicación según MINTIC.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 1. Criterios de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración 2. Niveles de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

6. IDENTIFICACIÓN DE RIESGOS

ID	ESCENARIO DE RIESGO	AMENAZA	VULNERABILIDAD
R_1	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de operadores de botnets	Operadores de Botnets	Deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
R_2	Compromiso de la disponibilidad, integridad o confidencialidad de los endpoints fijos, endpoints portátiles o endpoints estaciones ingeniería, por acción de operadores botnets.	Operadores de Botnets	Deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos
R_3	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers	Hackers	Falta en controles de seguridad informática en la gestión de las redes
R_4	Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers	Hackers	Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información

R_5	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción de hackers	Hackers	Falta en controles que garanticen la adecuada gestión de las vulnerabilidades técnicas
R_6	Afectación de la integridad, disponibilidad y confidencialidad del servicio de correo electrónico institucional, por acción de phishing, debido a una alta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática	Phishing	Falta o deficiencia en la toma de conciencia, educación y formación en la seguridad informática
R_7	Afectación de la integridad, disponibilidad y confidencialidad de los servidores de bases de datos, por acción de atacante interno	Atacante interno(insider)	Falta o deficiencia en controles sobre el acceso a redes y servicios en red

Tabla 1. Identificación de riesgos

De acuerdo con los riesgos identificados y las escalas propuestas por el Departamento Administrativo de la Función Pública, se realizó la actividad de valoración de los riesgos. A continuación, se presenta el mapa de riesgos producto de la aplicación de los controles identificados.

	MAPA DE RIESGOS EN SEGURIDAD INFORMÁTICA FRENTE A CIBERAMENAZAS						
Probabilidad de ocurrencia	Casi seguro	5					
	Probable	4					
	Posible	3		R_2	R_5, R_6	R_4, R_7	
	Improbable	2			R_1, R_3		
	Rara vez	1					
			1	2	3	4	5
			Insignificante	Menor	Moderado	Mayor	Catastrófico
			Impacto de materialización				

Tabla 2. Mapa de Riesgos

7. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN POR CATEGORÍAS FRENTE A CIBERAMENAZAS.

Según lo expuesto en la guía para la administración del riesgo y el diseño de controles en entidades públicas por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de seguridad y privacidad de la información enfocado en la seguridad informática sobre los activos de tecnologías de información frente a ciberamenazas. En atención a lo anterior, se describen las actividades más relevantes orientadas al tratamiento de riesgos de seguridad y privacidad de la información desde el enfoque de seguridad informática frente a ciberamenazas:

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN POR CATEGORÍAS FRENTE A CIBERAMENAZAS		
N°	**Descripción de la actividad**	**Responsable**
1	Adquisición de Controles de Seguridad Informática frente a Ciberamenazas	Ingeniero de sistemas encargado
2	Implementación de Controles de Seguridad Informática frente a Ciberamenazas	Ingeniero de sistemas encargado
3	Seguimiento a la Operación de los Controles de Seguridad Informática frente a ciberamenazas	Ingeniero de sistemas encargado

Tabla 3. Plan de tratamiento de riesgo

El desarrollo de las actividades mencionadas, para lograr su ejecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo corporativo que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

ELABORADOR POR	**FECHA**	**VERSIÓN**
Ingeniero de Sistemas Eider Ojeda	23/6/2022	1.0