EMPRESA DE SERVICIOS PUBLICOS DE LEBRIJA E.S.P.

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

VIGENCIA 2024

DR. EDUARDO VASQUEZ ZORRO
GERENTE

Lebrija, Diciembre 2022

INTRODUCCIÓN

La información que hace parte de la Empresa de Servicios Públicos de Lebrija ESP es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Empresa, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Empresa del Estado. De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (en adelante MSPI), un tema Decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones.

1. OBJETIVOS

Realizar un análisis y valoración de los riesgos de seguridad de la información en cuanto al impacto y la probabilidad de ocurrencia para la Empresa de Servicios Públicos de Lebrija ESP.

Especificar la metodología de gestión de riesgos de seguridad y privacidad de la información contemplando: Identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en la Empresa de Servicios Públicos de Lebrija ESP teniendo en cuenta los lineamientos descritos en Modelo de seguridad de la información.

2. ALCANCE

La Guía Metodológica de Análisis de Riesgos de Seguridad y Privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información de la Empresa de Servicios Públicos de Lebrija ESP.

3. DEFINICIONES

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Autenticidad: Propiedad de que una Empresa es lo que afirma ser. Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

4. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Definición del Riesgo

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias". De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información la empresa.

De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital1, la estrategia de administración de riesgos para el flujo de la información en los procesos busca diseñar una metodología ligera enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información.

4.1 Riesgos de Seguridad Digital

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico.

4.2 Riesgos de Privacidad

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

4.3 Incidente de Seguridad de la Información

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como "Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer Las actividades y vulnerar la seguridad"; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información

5. ANÁLISIS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA EMPRESA

Se identifican los activos de información, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada a los factores. En la gestión de valoración del activo, se consideran los siguientes aspectos:

ACTIVOS	DESCRIPCIÓN
Activos Esenciales	Datos importantes o vitales para la Administración de la Empresa: Aquellos que son esenciales, imprescindibles para la continuidad de la Empresa; es decir que su carencia o daño afectaría directamente a la Empresa, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). Datos Clasificados o Calificados: Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	Es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. Ejemplo: Copias de Respaldo, Datos de Configuración, Contraseñas, Datos de Control de Acceso, Registros de Actividad, Código Fuente, entre otros.
Hardware / Infraestructura	Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la Empresa, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Por Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Equipos de Respaldo, Periféricos, Dispositivos Biométricos, Impresoras, Escáneres, Equipos Soporte de la Red , IP interconectados con tecnología Grandstream, IP y 4 NVR para los registros y administración, Lector de huellas biométrico IP para control de acceso, arquitectura Ethernet Router Board Mikrotic RB1100Ahx2.
Software / Aplicaciones Informáticas	Gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. Ejemplo: Estándar, Navegador, Servidor, Correo Electrónico, Servidor de Correo Electrónico, Sistemas de Gestión de Bases de Datos, Software SOUL GT, Ofimática, Antivirus, Sistema Operativo, Backup o Respaldo.

Servicios	Funciones que permiten suplir una necesidad de los usuarios (del servicio). Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de la entidad (altas y bajas de usuarios del sistema).
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Contratistas, Proveedores.
Soportes de Información	Dispositivos físicos electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo. Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red, Memorias USB, CDROM, DVD, Cinta Magnética, Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso.

Se establecen los niveles de riesgos teniendo una clasificación propia para de la empresa:

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Acción Requerida
Riesgo Extremo	Evadir el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Moderado	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo
Riesgo Bajo	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones defectivas y preventivas.

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

Producto de los análisis de riesgos de seguridad y privacidad de la información, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las Características de confidencialidad, integridad y disponibilidad de la misma, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

7. PLAN DE ACCIÓN VIGENCIA 2024

ITEM	DESCRIPCIÓN	ENTREGABLE	FECHA
Actualizar matriz de riesgos	Realizar la identificación de los riesgos de la información	Matriz de riesgos	Diciembre 10 DE 2024
Calificación de impacto de los riesgos	Definir tipos de efectos o impactos	Matriz de riesgos	Diciembre 10 DE 2024
Evaluar los riesgos	Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente	Matriz de riesgos	Diciembre 10 DE 2024

El presente plan fue aprobado por el comité institucional de gestión y desempeño según acta de trabajo 001-2024 del día 29 de enero de 2024.

Dr. EDUARDO VASQUEZ ZORRO
Gerente

Apoyo:
Sergio Mauricio Ramírez
Contratista de apoyo de control interno