ANEXO RESOLUCION N°0035 DE 2019

PLAN DE GESTION DEL RIESGO EN LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Empresa de Desarrollo Urbano de Armenia LTDA - EDUA

INTRODUCCIÓN

Actualmente las entidades reconocen la importancia de la información en sus procesos productivos, por tanto la necesidad de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

La Empresa de Desarrollo Urbano de Armenia Ltda. EDUA decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad**: Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad**: Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad**: propiedad que la información sea accesible y utilizable en el momento que se requiera.

OBJETIVOS

Objetivo General: Diseñar e implementar un plan de gestión de riesgos de seguridad y privacidad que permita mitigar los riesgos de pérdida de activos de información en la Empresa de Desarrollo Urbano de Armenia LTDA.

Objetivos Específicos

- Determinar el alcance del plan de gestión de riesgos de la

seguridad y privacidad de la información.

- Especificar los activos sujetos de protección en la Entidad.
- Identificar las principales amenazas que afectan a los activos de información.
- Proponer plantillas o formatos de reportes para tener un control de situaciones presentadas en la Entidad.
- Clasificar los eventos que amenacen la disponibilidad, veracidad y confidencialidad de la información y gestionarlos con eficacia.
- Proponer soluciones para mitigar los riesgos a los que está expuesto cada activo de información.
- Evaluar el nivel de riesgo actual frente al impacto generado después de ejecutar el plan de gestión de riesgos de la seguridad de la información.

ALCANCES Y LIMITACIONES

ALCANCES

- Conseguir que el equipo de la Empresa de Desarrollo Urbano de Armenia LTDA. tenga el compromiso para emprender la implementación del plan de gestión de los riesgos de la seguridad de la información.

- Sensibilizar y capacitar al personal de la Entidad en el plan de gestión de riesgos de la seguridad de la información.

- Delegar funciones para apoyar y asesorar el proceso de diseño e implementación del plan de gestión de riesgos de la información.

LIMITACIONES

- Presupuesto insuficiente para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Empresa de Desarrollo Urbano de Armenia LTDA.

IMPORTANCIA DE LA GESTIÓN DE RIESGOS

- Debido a que los software, sistemas de información y avances tecnológicos vienen siendo implementados en las empresas del mundo, y con ellos mayor velocidad en el procesamiento de información y disponibilidad de la misma, se debe dar mayor prioridad a salvar, proteger y custodiar los activos de información para brindar disponibilidad, veracidad y confidencialidad.

- La Empresa de Desarrollo Urbano de Armenia LTDA. propende por cumplir los lineamientos trazados en la Ley de Transparencia 1712 de 2014 del Gobierno Nacional y Gobierno Digital que sugieren actividades a nivel de las entidades públicas para que se ejecuten modelos y estándares en aras de brindar seguridad y protección a la información.

- Una entidad sin un plan de gestión de riesgos está expuesta a perder su información dado por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas.

- Todas las organizaciones deberían implementar planes para gestionar los riesgos que afecten la seguridad y privacidad de la información desde software, tecnologías y específicamente en las unidades de datos, teniendo en cuenta que en la actualidad las amenazas más reiteradas son ataques dirigidos a los sistemas empresariales, afectando la disponibilidad, veracidad y confidencialidad de la misma.

- Todo tipo de ataques o desastres que pongan en peligro la integridad de la información de la Entidad, deben estar

contemplados y ser tratados bajo el plan de gestión de riesgos que permitan la normal continuación del negocio.

DEFINICION GESTIÓN DEL RIESGO

- La gestión del riesgo se define como el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse.

VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

IDENTIFICACIÓN DEL RIESGO

1. Riesgo Estratégico: Tiene que ver con la manera en cómo se administra la Entidad. El manejo del riesgo estratégico tiene que ver con asuntos misionales y el cumplimiento de los objetivos estratégicos, la definición de políticas y estructura de la organización por parte de la alta gerencia.

2. Riesgos de Imagen: Tipo de percepción y niveles de confianza por parte de la ciudadanía hacia la institución.

3. Riesgos Operativos: Son los riesgos que se originan a partir del

Dirección Carrera 16 17-00, piso 5 Tel – (6)744 35 67 744 71 00 Ext.502 CP.630004
Correo Electrónico: gerencia@edua.gov.co

funcionamiento y operatividad de los sistemas de información de la Entidad, de la ejecución de los procesos y de la articulación entre las dependencias.

4. Riesgos Financieros: Tienen que ver con el manejo de los recursos de la Entidad como planeación presupuestal, pagos, ejecución presupuestal, elaboración de estados financieros, manejos de excedentes de tesorería y el manejo de los bienes.

5. Riesgos de Cumplimiento: Están relacionados con la capacidad que tiene la Entidad para cumplir con las exigencias legales, contractuales, de ética pública y en general con el compromiso con la comunidad en congruencia con su misión empresarial.

6. Riesgos de Tecnología: Tienen que ver con la infraestructura tecnológica con que cuenta la Entidad para satisfacer los requerimientos actuales y futuros.

SITUACIONES NO DESEADAS

- Pérdida de información ya sea de manera incidental o premeditada.
- Alteración de claves de inicio de sesión ya sea por parte de los computadores de las estaciones de trabajo y/o desde los servidores supeditados por software malintencionado.
- Débil velocidad de conexión al servicio internet tanto que impida la navegación u operatividad de los sistemas de información.
- Avería de equipos de cómputo u obsolescencia de los mismos.
- Atrasos en la entrega de información.
- Negligencia en asistencia técnica.
- Manipulación indebida de información.
- Víctimas de algún tipo de virus informático.
- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión.
- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.

PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD

Dirección Carrera 16 17-00, piso 5 Tel – (6)744 35 67 744 71 00 Ext.502 CP.630004
Correo Electrónico: gerencia@edua.gov.co

DE LA INFORMACIÓN.

- Garantizar el cumplimiento de los requisitos de seguridad de la información para generar un producto o servicio que dependa de datos
- Diagnosticar las fortalezas y debilidades que atañen a los riesgos de la Empresa de Desarrollo Urbano de Armenia LTDA.
- Construcción de un plan de prevención y acción ante incidentes previsibles y no previsibles.
- Brindar el respectivo respaldo al modelo de seguridad de la información de la Entidad.
- Definir los alcances de la Entidad con base en los riesgos de la seguridad de la información.

IDENTIFICACIÓN DEL RIESGO

ANALISIS DE VULNERABILIDADES

DESCRIPCIÓN DE VULNERABILIDADES

Si tenemos en cuenta que estar expuesto cuando se presenta un fenómeno amenazante, o ser incapaz de reponerse después de que ha ocurrido un desastre, la Empresa de Desarrollo Urbano de Armenia LTDA. no es la excepción y en una inspección a nivel físico y lógico se identificaron los siguientes riesgos:

GERENCIA:

En gerencia se cuenta con un equipo de cómputo que presenta constantes fallas que en cualquier momento puede presentar un daño y generar perdida

de información, además se conecta a internet mediante una red WiFi, por tanto, el riesgo que se podría presentar es pérdida súbita del servicio dada la distancia del equipo con respecto al enrutador y las paredes que la señal debe evadir

ÁREA ADMINISTRATIVA Y FINANCIERA

Se encuentran cables que sobresalen de la pared e incluso tienen el riesgo de quedar debajo de los pies del funcionario, esto da pie para generar un daño tanto físico como de funcionamiento lógico ya sea de acceso a la red o del mismo equipo de cómputo.

AREA DE CONTROL INTERNO

La canaleta que protege los cables en el puesto de trabajo de la Direccion de Control Interno se encuentra en mal estado y por ende los cables están sueltos hay probabilidad de que estos cables interfieran con el estabilizador o sean tocados por la funcionaria, además el equipo presenta lentitud y fallas que podría generar perdida de la información.

ÁREA JURÍDICA

Se encuentra que el Director trabaja en un portátil con acceso a wifi el cual presenta obsolencia y lentitud, además el puesto de trabajo presenta cables y humedades en el puesto contiguo.

ÁREA TÉCNICA

Se encuentran cables que sobresalen de la pared e incluso tienen el riesgo de quedar debajo de los pies del funcionario, esto da pie para generar un daño tanto físico como de funcionamiento lógico ya sea de acceso a la red o del mismo equipo de cómputo.

El ingeniero contratista de obras actualmente utiliza un computador portátil de su propiedad el cual se conecta a internet mediante una red WiFi, por tanto, el riesgo que se podría presentar es pérdida súbita del servicio dada la distancia del equipo con respecto al enrutador y perdida de la información si no se realizan las copias de seguridad y no se solicita por el supervisor copia de la información digital de la información contractual en caso de no continuar con la prestación de sus servicios.

RIESGOS GENERALES:

Las políticas y normas de seguridad de la información no se han socializado con todo el personal, además de ello, se evidencia el incumplimiento de las

políticas de seguridad informática como reglas adicionales básicas del cuidado tanto de los equipos de cómputo como de la información física y digital, algunas son:

- No se cuenta con presupuesto asignado para la adquisición de equipos de cómputo en la entidad y con los que se cuenta son de propiedad del Municipio los cuales pueden ser requeridos en cualquier momento.
- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos o residuos pueden llegar a afectar los equipos de cómputo.
- La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la entidad.
- No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados.
- No se cuenta con presupuesto asignado para la adquisición de equipos de cómputo en la entidad y con los que se cuenta son de propiedad del Municipio los cuales pueden ser requeridos y quedar en la entidad sin equipos.

PROPUESTA DE SEGURIDAD

- Se deben ajustar los cables que sobresalen de la pared y de las divisiones de área generalmente ubicados debajo de los escritorios de los funcionarios.
- Revisar y organizar las conexiones eléctricas de la Entidad que requieran una intervención.
- Inspeccionar y cambiar las canaletas que se encuentren en mal estado.
- Se sugiere determinar una caja de seguridad para guardar el disco externo de la Entidad, el cual contiene las copias de los activos de información
- Socializar las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática como reglas básicas de cuidado de los equipos.
- Los servidores y equipos de comunicaciones deben estar acomodados en un bastidor adecuado para ello y en un espacio dedicado y acondicionado para mantener los activos en un ambiente propicio.

7. SEGUIMIENTO, MEDICION, ANALISIS Y EVALUACION

La EMPRESA DE DESARROLLO URBANO DE ARMENIA LTDA. “evaluará el desempeño del plan de gestión de riesgos de seguridad y privacidad de la información”, por medio de un monitoreo esencial para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables de los procesos, la Oficina de Control Interno y la Oficina de Tecnologías de la Información, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.

8. CONCLUSIONES

El seguimiento constante a los procesos y la implementación del plan de mitigación de riesgo de seguridad de la información deben ser ejecutados, monitoreados y actualizados frecuentemente.

Es indispensable implementar el plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad.

Dirección Carrera 16 17-00, piso 5 Tel – (6)744 35 67 744 71 00 Ext.502 CP.630004
Correo Electrónico: gerencia@edua.gov.co