INFORME DE SEGUIMIENTO DE MATRIZ DE SEGURIDAD DIGITAL

ALCALDIA MUNICIPAL DE GIRARDOT

OTIC

MAYO-AGOSTO

2021

GIRARDOT ES DE TODOS
Edificio Administrativo Alcaldía Municipal Cll.17 con Cra.11 Esquina. Piso (4)
Código Postal N° 252432 Girardot-Cundinamarca
sistemas@girardot-

INTRODUCCION

La Alcaldía Municipal de Girardot identifica la información como un componente indispensable para mantener la entidad en un buen manejo de su misión y tenerla orientada a su visión, razón por la cual es necesario establecer un marco en el cual se asegure la información de una manera adecuada, independientemente de la forma en la que esta sea manejada, procesada, transportada o almacenada.

Este documento surge como una herramienta institucional para realizar una valoración, seguimiento y control de los riesgos de seguridad digital de la alcaldía municipal de Girardot.

Las políticas y normas de seguridad de la información definidas por la alcaldía municipal de Girardot. Para la elaboración del mismo, se toma como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013, las recomendaciones del estándar ISO 27002:2013 y el Ministerio de las TIC.

Las políticas incluidas en este matriz se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la alcaldía municipal de Girardot y se convierte en la base para la creación de los controles, procedimiento y estándares definidos.

La seguridad de la información es una prioridad para la alcaldía municipal de Girardot y por lo tanto es responsabilidad de todos velar porque no se realicen actividades que contradigan cada una de estas políticas.

GIRARDOT ES DE TODOS
Edificio Administrativo Alcaldía Municipal Cll.17 con Cra.11 Esquina. Piso (4)
Código Postal N° 252432 Girardot-Cundinamarca
sistemas@girardot-

ALCANCE

Este documento consolida la información de los resultados del seguimiento de la ejecución de las actividades de control implementadas por cada una de las dependencias de la Alcaldía Municipal de Girardot.

VALORACION DE LOS RIESGOS DE SEGURIDAD DIGITAL

Previo la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información en los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad digital.

La valoración del riesgo de seguridad de la información consta de las siguientes actividades:

- **Análisis del Riesgo**
- **Identificación del Riesgo**
- **Evaluación del Riesgo**

ANALISIS DEL RIESGO

Para realizar el análisis del riesgo es necesario identificar cuáles son los riesgos:

1. Daños físicos en los equipos tecnológicos: son las averías o fallas causada a los equipos

2. Fraude y delitos electrónicos: fraude realizado a través del uso de una computadora o del internet.

3. Perdida de Información: Se puede producir por cualquier causa, una avería, un error humano, un borrado accidental o provocado, desastres naturales, incendios, golpes reparar disco duro etc. Las pérdidas de datos tienen su origen más frecuente en las averías físicas, seguido por el error humano.

4. Correos electrónicos de extraña procedencia: son un tipo de virus conocidos como Troyanos, los cuales contienen un programa dañino que se oculta en otro programa y produce efectos dañinos en el equipo y la información.

IDENTIFICACION DEL RIESGO

Determinar que podría suceder que cause una pérdida parcial o total, como, donde y cuando podría ocurrir la perdida.

Los riesgos se identifican como eventos o situaciones no deseadas, que se pretenden evitar.

EVALUACION DEL RIESGO

Después de analizar e identificar el riesgo, se pueden evaluar los riesgos, lo cual permite la adopción de medidas y la toma de decisiones necesarias para prevenir o mitigar que ocurran.

SEGUIMIENTO MATRIZ – VIGENCIA 2021

El seguimiento de las actividades de control se realizó por cada responsable del proceso. Este proceso implico recopilación de la información para cada control establecido.

RESULTADO

El seguimiento realizado a las actividades de control definidas se encuentran registradas en el Informe presentado **"SEGUIMIENTO A PLAN ANTICORRUPCIÓN Y**

ATENCIÓN AL CIUDADANO VIGENCIA 2021" en el seguimiento e informe de la Matriz de Riesgo de Seguridad Digital.

En el segundo semestre se realizó el seguimiento de los 4 Riesgos identificados en la Alcaldía Municipal de Girardot:

1. Daños Físicos en los Equipos Tecnológicos

1.1 Consumir alimentos en los puestos de trabajo:

La actividad de control fue retroalimentado el Manual de Políticas de Seguridad y Privacidad de la Información, por medio de la capacitación realizada el 11 de agosto del 2021, donde se explicó el cuidado que se debe tener con los quipos tecnológicos.
A la fecha no se ha reportado ningún tipo de daño en los equipos por derramamiento de líquidos o por consumo de alimentos.

1.2 Daño por el polvo y la humedad:

Por medio del oficio D.A.S.T.I.C.203.47 N 066-2021, se solicita a Almacén el Stock de materiales y herramientas tecnológicas para poder llevar a cabo los mantenimientos preventivos y correctivos. De todas formas, se cuentan con los técnicos de sistemas para brindar el soporte cuando sea requerido.

1.3 Falta de conciencia en el uso de los equipos tecnológicos:

Se realizó sensibilización por medio de una capacitación de Manual de Políticas de Seguridad y Privacidad de la información. Se explicó el respectivo manejo y cuido de los equipos tecnológicos que utilizan los funcionarios. A la fecha no se presenta ningún tipo de daño en los equipos.

1.4 Variaciones de voltaje y disponibilidad de energía:

Se solicita por medio del oficio D.A.S.T.I.C.203.47 N° 066-2021 a Almacén para confirmar la cantidad de equipos tecnológicos que cuentan con UPS y/o estabilizador

2. Fraude y Delitos Electrónicos:

2.1 Falta de Seguridad en las entidades Bancarias:

Por medio del oficio D.A.S.T.I.C.203.47 N° 091-2021, se solicita a todas las entidades bancarias con las cuales la Alcaldía Municipal maneja cuentas, los protocolos de seguridad bancaria. Todo esto con el fin de brindar la información al personal.

2.2 Falta de Conocimiento en temas de seguridad digital:

Se realiza retroalimentación sobre el Manual de Políticas de Seguridad y privacidad de la Información el día 11 de agosto del 2021.

3. Perdida de Información:

3.1 Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo:

Se realiza retroalimentación el día 11 de agosto del Manual de Políticas de Seguridad y Privacidad de la Información. En el cual se hace énfasis de la importancia de cerrar y finalizar sesión, al igual que no se debe prestar el usuario. A la fecha no se ha reportado ningún tipo de perdida de información.

3.2 Ausencia de copias de seguridad:

Se capacitado a todas las dependencias como se debe realizar la copia de seguridad en la unidad red asignada se realizó 11 de agosto del 2021.

3.3 Ausencia de protección de virus: Se realiza la compra e instalación del antivirus

3.4 Ausencia de mecanismos de identificación y autentificación de los usuarios con aplicativos autónomos.

Se realizó la capacitación el 11 de agosto del 2021 sobre los formatos de creación de usuarios que están habilitados por calidad.

4. Correos Electrónicos de extraña Procedencia

4.1 Ausencia de Políticas para el uso correcto de correo electrónico:

Se realiza capacitación el día 11 de agosto del presente año del Manual de Políticas de Seguridad y Privacidad de la Información. En el cual se explica el manejo y uso adecuado del correo electrónico.

CONCLUSIONES:

- Es importante realizar la capacitación del Manual de Políticas y Seguridad de la Información de forma periódica, para reforzar y capacitar al nuevo personal, que ingresa de forma constante.

- Es necesario que las dependencias que manejan software independiente, tengan algún tipo de control en la creación de usuarios y la autenticación de los mismos, todo esto con el fin de garantizar seguridad en el manejo de la información.

- Es necesario como parte del control, monitoreo y seguimiento de la Matriz de Riesgo de Seguridad Digital. Por lo tanto, las acciones que se integran dentro de los controles deben permitir a la entidad poder identificar los diferentes tipos de amenazas y poder implementar controles para mitigarlos y/o evitarlos.