Emsercota S.A.

EMPRESA DE SERVICIOS PÚBLICOS

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

INTRODUCCIÓN

En la gestión de riesgos de seguridad de la información se tratan aquellos procesos que ayudan a reducir las pérdidas y proporcionan protección a los datos en información y permiten dar a conocer las falencias y debilidades que se tienen en los ciclos de los servicios.

Por esta razón en importante contar con un plan de riesgos que permita dar continuidad al funcionamiento de la administración, debido a esto se desarrolla un análisis de riesgo de seguridad de la información aplicado en la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP.

Se busca identificar las respectivas amenazas, medir los riesgos existentes y sugerir las acciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

Este plan da una proyección que permite identificar los niveles de riesgo de la información y como está la seguridad existente, buscando incentivar a las personas involucradas a continuar con el uso de las normas y procedimientos pertinentes a la seguridad de la información y recursos.

1. Objetivos

1.1 Objetivo General

Desarrollar un plan de gestión de seguridad y privacidad de la información que tenga como resultado la disminución de los riesgos de pérdida de información en la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP.

1.2 Objetivos Específicos

- Plantear modelos de reportes para su uso en las incidencias presentadas en la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP.
- Gestionar los eventos de seguridad de la información para identificar si es necesario clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Identificar las principales amenazas que afectan la seguridad de la información de la administración.
- Proponer soluciones para minimizar los riesgos a los que se expone la información
- Evaluar el impacto generado después de implementar el plan de gestión de seguridad de la información

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

- Comprometer a la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP, para iniciar la implementación del plan de gestión del riesgo en la seguridad de la información.
- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

2.2 LIMITACIONES

- Crear el rubro del presupuesto necesario para apoyar los planes de acción de TI dentro de la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP.
- Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP.

3. GESTIÓN DE RIESGOS

3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

A nivel mundial dentro de las organizaciones cada vez de da mayor prioridad a salvaguardar, custodiar y proteger los activos de información ya que gracias a los avances tecnológicos y los sistemas de información tiene estas implementaciones

La Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP, siguiendo los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno Digital impulsando actividades que brinden seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Todas las organizaciones deben implementar planes para gestionar los riesgos que afectan la información, sus tecnologías y activos, debido a que se es común

evidenciar ataques dirigidos a software empresarial, y esto da como resultado problemas en la disponibilidad e integridad de la información.

Por esta razón se debe prevenir todo tipo de ataques o desastres, ya que los costos de recuperación son mayores a los de prevención y afectan la continuidad del negocio al sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP, es necesario diseñar un plan e iniciar las prácticas de las normas y políticas de seguridad para asegurando la continuidad de los servicios.

3.2 DEFINICION GESTIÓN DEL RIESGO

La definición de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización".

3.3 IDENTIFICACIÓN DEL RIESGO

1. Riesgo Estratégico: Asociado a como se administra la Entidad, se enfoca en asuntos relacionados con la misión y el cumplimiento de los objetivos estratégicos, definición de políticas, diseño y conceptualización de la entidad.

2. Riesgos de Imagen: Relacionados a cómo percibe la ciudadanía hacia la institución y que nivel de confianza le tienen.

3. Riesgos Operativos: Son riesgos sobre el funcionamiento y operatividad de los sistemas de información institucionales, de los procesos, la estructura y la articulación entre dependencias dentro de la administración.

4. Riesgos Financieros: Relacionados con los recursos de la entidad entre estos la ejecución presupuestal, la elaboración de los estados financieros entre otros.

5. Riesgos de Cumplimiento: Asociados en el compromiso de la entidad ante la comunidad de acuerdo a la misión establecida.

6. Riesgos de Tecnología: Relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

3.4 SITUACION NO DESEADA

- Manipulación incorrecta de información
- Hurto de información o de equipos informáticos.
- Perdida de información por intrusión en las instalaciones, por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de internet.
- Daño de equipos y de información
- Atrasos en la entrega de información
- Atrasos en asistencia técnica
- Fuga de información

4. ORIGEN DEL PLAN DE GESTION

Debido a que la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP, no cuenta con área de sistemas conformada y se evidencia que no existen procesos asignados a dicha área además otras flaquezas que se encontraron en el sistema actual, se hace necesario la creación de un plan de gestión de riesgos de seguridad de la información para proteger el activo más valioso para la entidad; la información.

Es necesario que la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP, cumpla con los requisitos necesarios establecidos por el Gobierno Nacional y Min Tic para entregar la información de manera oportuna y eficiente ante entes externos y las dependencias propias de su administración

4.1 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

Preparación de un plan de respuesta a incidentes.

Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.

Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

5. ANALISIS DE VULNERABILIDADES

5.1 DESCRIPCIÓN DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Empresa de Servicios Públicos de Cota EMSERCOTA SA ESP se evidencian otras amenazas como son:

1. Se requiere licencias de software de sistemas operativos y ofimática para los PC de los funcionarios.
2. Se requiere software de Antivirus licenciado para los equipos que cuentan con Sistemas de Información local en su PC.
3. Los PC de los funcionarios sufren de lentitud al ejecutar los programas requeridos para su trabajo.
4. No se cuenta con el servicio de respaldo para la información crítica de la Entidad.
5. Se requiere realizar pruebas de vulnerabilidades de seguridad en la red protegida de la Entidad.
6. Se debe ordenar el cableado de la data center principal ya que la red existente esta con diferentes categorías.
7. Los puntos de red ubicados en las oficinas no son suficientes, se implementan nuevos según se presenta la necesidad.
8. Aunque se creó el cargo de Técnico Administrativo de Sistemas en la Empresa, se hace necesario seguir fortaleciendo de manera trasversal en todos los procesos la protección y tratamiento de la seguridad y Privacidad de la información.
9. La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.

10. No hay control en el uso de memorias portátiles en los equipos de la empresa, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
11. Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en la empresa.
12. No existe un Firewall para la red inalámbrica de la empresa.
13. No existen procesos de copias de seguridad establecidos.
14. Se requiere que la pagina web de la empresa cuente con todas las normas exigidas por los entes de control y además que sea interactiva con los usuarios que la consulten.

6. Plan de acción:

1. Licencias de Software de Sistemas Operativos y Ofimática:

Adquirir licencias legítimas de software de sistemas operativos (como Windows) y ofimática (Microsoft Office). Esto garantizará el cumplimiento de la ley y la optimización de recursos.

2. Software Antivirus Licenciado:

Adquirir una solución antivirus que cubra todos los equipos con sistemas de información local con el fin prevenir infecciones de malware, proteger datos y garantizar el cumplimiento de políticas de seguridad.

3. Lentitud en los PC:

Realizar un diagnóstico de los equipos (hardware y software). Mejorar el rendimiento puede implicar actualizar el hardware (memoria RAM, discos duros SSD) y optimizar el software mediante la eliminación de programas innecesarios o

la configuración adecuada del sistema operativo, también considerar la compra de equipos con especificaciones actuales.

4. Falta de Respaldo de Información Crítica:

Contratar el servicio de almacenamiento en la nube o local, garantizando la recuperación en caso de desastre. La solución de respaldo debe ser periódicamente probada para asegurar que los datos pueden ser recuperados de forma eficiente.

5. Pruebas de Vulnerabilidades en la Red:

Contratar un servicio de auditoría de seguridad que realice pruebas de penetración y escaneo de vulnerabilidades de forma regular. Esto ayudará a identificar posibles puntos débiles en la red antes de que sean explotados por cibercriminales.

6. Desorden en el Cableado del Data Center:

Realizar una reestructuración del cableado en el data center, asegurando que todos los cables estén organizados y clasificados por categorías. El uso de racks y etiquetado adecuado mejorará la gestión y la seguridad física del centro de datos.

7. Insuficiencia de Puntos de Red en Oficinas:

Evaluar el diseño de la red y, si es necesario, instalar nuevos puntos de red conforme se requiera. Asegurarse de que el cableado sea adecuado para soportar los dispositivos y aplicaciones que los funcionarios necesitan.

8. Fortalecimiento de la Seguridad y Privacidad en Todos los Procesos:

Capacitar a todo el personal en buenas prácticas de seguridad y privacidad de la información.

9. Información en Memorias o Discos Duros Portátiles:

Implementar protocolos estrictos de manejo de datos sensibles. Usar almacenamiento cifrado y soluciones de gestión de dispositivos (MDM) para controlar el uso de memorias USB y discos duros portátiles.

10. Falta de Control en el Uso de Memorias Portátiles:

Implementar un sistema de control que permita gestionar y restringir el uso de memorias USB y otros dispositivos externos en los equipos de la empresa. Establecer protocolos claros sobre el uso y la autorización para conectar dispositivos externos.

11. Desconocimiento de Seguridad y Privacidad:

Implementar campañas de sensibilización en seguridad de la información para todos los empleados. Asegurarse de que comprendan las amenazas comunes, como el phishing, y las mejores prácticas para proteger la información sensible.

12. Falta de Firewall para la Red Inalámbrica y la intranet:

Instalar un firewall dedicado a proteger la red inalámbrica e intranet de la empresa. Configurar la red Wi-Fi con protocolos de seguridad robustos.

13. Ausencia de Copias de Seguridad Establecidas:

Adquirir un sistema de para realizar las copias de seguridad automatizadas que cubra todos los datos relevantes, tanto a nivel local como en la nube. Crear un calendario regular de pruebas de restauración de respaldos para garantizar que los datos pueden ser recuperados correctamente.

14. Página Web No Cumple con Normas y No es Interactiva:

Rediseñar la página web para cumplir con las normativas de accesibilidad y las exigencias de los entes reguladores. Además, asegurar que la página sea interactiva y fácil de usar, con formularios en línea, encuestas y otros elementos que faciliten la interacción con los usuarios.

15. Cambio de Protocolo delPV4 a IPV6:

Contratar una auditoría para identificar los componentes de la infraestructura de red que deben actualizarse, configurarse o reemplazarse para soportar IPv6.

ANA AIDA PARDO CARRILLO
Subgerente Corporativo

YAMIR GEOVANNY QUEVEDO AGUDELO
Técnico Administrativo Sistemas

Proyecto: Yamir Geovanny Quevedo Agudelo – Técnico Administrativo sistemas