**Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

Informe Ejecutivo

UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PUBLICOS

Bogotá D.C. Julio de 2018

Contenido

[1. Objetivo del Documento 3](#_Toc521501818)

[2. Metodología de Gestión de Riesgo 3](#_Toc521501819)

[2.1 Análisis y Evaluación de Riesgos de Seguridad de la Información 3](#_Toc521501820)

[2.1.1 Identificación de la Vulnerabilidades 3](#_Toc521501821)

[2.1.2 Identificación de Riesgos 4](#_Toc521501822)

[2.1.3 Clasificación del Riesgo 4](#_Toc521501823)

[2.2 Tratamiento del Riesgo 5](#_Toc521501824)

[3. Términos y Definiciones 9](#_Toc521501825)

# Objetivo del Documento

Definir el proceso mediante el cual se realizará la gestión de riesgos de seguridad de la información en la Unidad Administrativa Especial de Servicios Públicos (UAESP), la cual debe incluir, amenazas, vulnerabilidades, riesgos, controles, niveles aceptables de riesgo y el tratamiento de riesgos.

Este documento fue presentado y aprobado el 8 de agosto en el Comité de Seguridad de la Información y Gobierno Digital.

# Metodología de Gestión de Riesgo

La metodología de gestión de riesgos ofrece para la UAESP un método sistemático para analizar los riesgos derivados de los procesos misionales y del uso de las tecnologías de la información y comunicaciones, con el objetivo de descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control y así preparar a la entidad para un proceso de evaluación, auditoría, certificación o acreditación, según corresponda.

# 2.1 Análisis y Evaluación de Riesgos de Seguridad de la Información

Las amenazas son de origen natural o humano y pueden ser accidentales o deliberadas, algunas amenazas pueden afectar a más de un activo generando diferentes impactos.

# 2.1.1 Identificación de la Vulnerabilidades

Las vulnerabilidades de los activos de información son debilidades que son aprovechadas por amenazas y generan un riesgo. Una vulnerabilidad que no tiene una amenaza asociada puede no requerir de la implementación de un control; sin embargo, es necesario identificarla y monitorearla.

Es importante tener en cuenta que un control mal diseñado e implementado puede constituir una vulnerabilidad.

# 2.1.2 Identificación de Riesgos

Los riesgos en seguridad de la información se identifican mediante las pruebas de seguridad, identificación por parte de los funcionarios quienes tienen claridad y han experimentado la materialización de algunos riesgos en sus procesos y finalmente por la experiencia de los consultores.

# 2.1.3 Clasificación del Riesgo

Durante el proceso de identificación del riesgo se hace una clasificación de estos teniendo en cuenta los siguientes conceptos:

**Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

**Riesgos Operativos:** Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

**Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda entidad.

**Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

**Riesgos de Tecnología:** Se asocian con la capacidad de la Entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporte el cumplimiento de la misión.

# 2.2 Tratamiento del Riesgo

En concordancia y alineación con los Niveles de Riesgos, las acciones requeridas se complementan en la tabla I:

Tabla I

****

El mapa de riesgos contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la Entidad, a continuación, se describen los siguientes:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vulnerabilidades** | **Amenazas** | **Riesgos** | **Riesgo zona NO aceptable** | **Clasificación Tipo de Riesgo** | **Controles Por Implementar** |
| Data Center sin piso falso | Inundación | Pérdida de la información  |  | Riesgo Operativo | **CTRL 008** |
| Usuarios por defecto y/o Contraseñas por defecto o débiles | Acceso no autorizado | Fuga de Información |  | Riesgo Tecnológico | **CTRL 001** |
| Política de acceso y ubicación a equipos de trabajo no existente/no difundida  | Daño de equipos | Pérdida de información |  | Riesgo Estratégico | **CTRL 002** |
| Política de acceso y ubicación de equipos de trabajo no existente/no difundida  | Falla eléctrica | Daño de equipos |  | Riesgo Estratégico | **CTRL 003** |
| Falta de sensibilización en el uso de contraseñas seguras para el acceso a los sistemas de información (débil control de Acceso del Equipo) | Vida útil del equipo | Decreto 4175 de 2011 - Directiva 0013 de 2005 Procuraduría - Decreto 1687 DE 2010 - Numeral A12.4.4 ISO 27001 |  | Riesgo Estratégico | **CTRL 001** |
| NO se realiza mantenimiento preventivo a estaciones de trabajo | Fallas físicas, lógicas y/o humanas | Pérdida de información |  | Riesgo Tecnológico | **CTRL 004** |
| No se realiza mantenimiento físico preventivo a servidores | Derrame de alimentos en información física o lógica | No disponibilidad del servicio  |  | Riesgo Tecnológico | **CTRL 004** |
| Consumo de alimentos en el puesto de trabajo | Incidentes de seguridad y delitos informáticos | Pérdida de la confidencialidad de la información |  | Riesgo Operativo | **CTRL 006** |
| No se cuenta con plan de continuidad de negocio o DRP documentado y probado para dar continuidad al servicio de UAESP o de la Oficina de tecnologías de la información | Ataques de hombre en el medio / Sniffers | Pérdida o Fuga de Información |  | Riesgo Estratégico | **CTRL 008** |
| Servicios, herramientas o protocolos desactualizados (PHP, Apache, SSL, Oracle) | Fallo en los sistemas de información | Perdida de Información |  | Riesgo Tecnológico | **CTRL 009** |
| No hay control de acceso a la red alámbrica para visitantes | Acceso No Autorizados  | Pérdida de información / Fuga de información |  | Riesgo Tecnológico | **CTRL 010** |
| Información de prueba para desarrollo sin política o datos sin transponer | Desarrolladores y administradores de aplicativos | Fuga de la información |  | Riesgo Estratégico | **CTRL 011** |
| No se cuenta con políticas de transporte de información en medios magnéticos. | Acceso no autorizado | Fuga de información,  |  | Riesgo Estratégico | **CTRL 025** |
| Desarrollo o cambios de sistemas de información sin un procedimiento documentado | Acceso no autorizado / Errores de manipulación | Pérdida de la confidencialidad, integridad y/o disponibilidad de la información |  | Riesgo Estratégico | **CTRL 011** |

De la anterior tabla se evidencia la siguiente información:

Cantidad Riesgos Identificados: **14**

Cantidad Riesgo que se encuentran en Zona no aceptable y que deberán ser tratados: **2**

Clasificación de los riesgos con los siguientes resultados:

Riesgos estratégicos: **7**

Riesgos operativos: **2**

Riesgos tecnológicos: **5**

La definición de los controles a implementar son los siguientes:

**CTRL 001:** Establecer y supervisar el uso de contraseñas seguras el cual debe incluir, directorio activo, aplicaciones que exijan el uso de contraseñas fuerte y sensibilización sobre el buen uso al personal.

**CTRL 002:** Establecer, difundir y supervisar una política de uso adecuando de equipos, ubicación y acceso.

**CTRL 003:** Establecer una revisión periódica del sistema de cableado.

**CTRL 004:** Establecer un procedimiento y un indicador para realizar seguimiento al mantenimiento preventivo de estaciones de trabajo y servidores tanto físico como lógico, si se cumple parcialmente complementar el procedimiento con ítems sin atender como estaciones de trabajo y mantenimiento físico a servidores.

**CTRL 006:** Establecer política de consumo de alimentos en zonas predispuesta para este fin, salvaguardando equipos y escritorios de trabajo.

**CTRL 008:** Documentar, establecer, implementar y realizar pruebas de un plan de continuidad del Negocio BCP que se ajuste a las necesidades de UAESP

**CTRL 009:** Realizar actualizaciones periódicas de software y verificación de parches.

**CTRL 010:** Fortalecer controles de acceso a la red, restringir o segmentar uso de redes para visitantes y empleados y usar contraseñas "fuertes".

**CTRL 011:** Documentar implementar y difundir políticas y/o procedimientos para el desarrollo de software.

Documentar implementar y difunfdir políticas y/o procedimientos para el desarrollo de software.

Documentar implementar y difunfdir políticas y/o procedimientos para el desarrollo de software.

**CTRL 025:** Establecer un procedimiento que garantice la seguridad de la información que deba ser transportada en medios magnéticos.

# Términos y Definiciones

* + **Activo:** Cualquier elemento que tenga valor para la organización y en consecuencia, deba ser protegido.
	+ **Amenazas:** Todo elemento con la capacidad de atentar contra la seguridad de la información.
	+ **Control:** Medida preventiva o correctiva ante la presencia de diferentes riesgos.
	+ **Vulnerabilidad de un activo:** Debilidades en cuanto a la seguridad de la información
	+ **Riesgo:** Posibilidad de que una amenaza aproveche una vulnerabilidad.
	+ **Riesgo Residual:** Valor de riesgo tras la aplicación de uno o varios controles
	+ **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
	+ **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
	+ **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
	+ **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida