1. **NOMBRE DE LA POLÍTICA:** Política de seguridad de la información para las relaciones con proveedores.

2. **OBJETIVO:** Proveer las directrices para que los activos manejados por proveedores estén cubiertos por las Políticas de Seguridad de la Información de la Unidad de Servicios Penitenciarios y Carcelarios USPEC evitando que los riesgos frente a la Confidencialidad, Integridad y Disponibilidad de la Información se materialicen.

3. **ALCANCE:** Inicia con la identificación de requisitos que deben cumplir los proveedores respecto a Seguridad de la Información y finaliza con el seguimiento, evaluación y control en la gestión de incidentes y/o eventos.

4. **INTRODUCCIÓN:** El documento describe la política de seguridad de la Información para la relación con proveedores en USPEC, quienes deben mantener la protección de los activos involucrados con base en el Sistema de Gestión de Seguridad de la Información. Se debe considerar que en la relación con un proveedor se pueden ver involucrados los diferentes tipos de activos: Información, Software, Hardware, Personas, Instalaciones, Procesos y Servicios, para lo cual será el proveedor quien defina los controles a implementar cuando los activos involucrados estén bajo su responsabilidad.

5. **DEFINICIONES:**

Activo: Cualquier elemento que tiene valor para la organización y que para Gestión de riesgos de seguridad de la información se consideran los siguientes tipos: información, actividades y procesos del negocio, software, hardware, personal, redes, organización y ubicación.

Amenaza: Causa potencial de incidente no deseado, el cual puede resultar en daño al sistema o a la Organización. [Fuente: ISO 27000].

Confidencialidad: Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.

Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada. [Fuente: ISO 27000].

Eventos: Presencia o cambio de un conjunto particular de circunstancias, que puede ser una o varias ocurrencias con una o varias causas. Un evento puede consistir en algo que no está sucediendo. [Fuente: ISO 31000].

Integridad: Propiedad de precisión y completitud.[Fuente: ISO 27000].

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado de los sistemas de información, con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización). [Fuente: ISO 31000].

Vulnerabilidad: debilidad identificada sobre un activo y que puede ser aprovechado por una amenazas para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información

6. CAPITULOS DE LA POLÍTICA:

6.1 Acuerdo de Confidencialidad

Debe ser firmado sin excepción alguna con todos los proveedores con los que se establezca cualquier tipo de intercambio de información y lo que debe señalar es que el acceso a los datos que hagan parte del servicio prestado a USPEC, solo pueden ser accedidos, leídos o conocidos por las personas y/o entidades que estén formalmente autorizadas. Este acuerdo trae consigo las penalizaciones con base en los daños potenciales ante la violación de la confidencialidad de la información.

6.2 Protección de Datos Personales

Se debe incluir dentro del Contrato una cláusula que haga referencia al cumplimiento de la Política de protección de datos personales de USPEC, documento que debe ser entregado al proveedor para su entendimiento y aceptación.

6.3 Personal Encargado del servicio

El dueño o responsable del proceso, debe garantizar que se realicen las validaciones correspondientes para que todos los funcionarios de la empresa proveedora, que manejan información provista por USPEC, estén cubiertos con las condiciones contractuales establecidas en referencia a las Políticas de Seguridad de la Información.

6.4 Gestión de Incidentes

Es obligación por parte de los funcionarios de la empresa proveedora el reporte de cualquier anomalía que sea detectada para que su tratamiento sea oportuno y se prevengan incidentes de Seguridad.

6.5 Requerimientos de Seguridad de Aplicaciones y/o Servicios

Si el proveedor es responsable por aplicaciones o servicios informáticos, éstos deben cumplir con los requerimientos de protección de la Confidencialidad, Integridad y Disponibilidad definidos por USPEC y debe demostrar con base en el activo que va a ser manejado, uno o más de los siguientes controles:

- ✓ **Monitoreo:** Estar en capacidad de brindar los mecanismos para detectar incidentes de seguridad de la información sobre el funcionamiento de la aplicación con el que se presta el servicio a USPEC. El nivel de detección se ajustará a los requerimientos del activo involucrado en el servicio.
- ✓ **Gestión de Vulnerabilidades:** Mantener un proceso de revisión permanente de las posibles vulnerabilidades en las aplicaciones que son responsabilidad del proveedor y establecer el proceso de asesoría hacia USPEC, con el fin de mitigar oportunamente los riesgos asociados con las vulnerabilidades identificadas.
- ✓ **Control de acceso:** Presentar los mecanismos de control de acceso a los servicios y los datos manejados con base en la **Política de Control de Acceso A3-PO-07** de USPEC.

- ✓ **Gestión de incidentes:** Contar con un esquema de identificación, reporte, escalamiento, tratamiento y documentación de los incidentes que se presenten en el funcionamiento de la aplicación o servicio prestado.
- ✓ **Soporte:** El proveedor debe contar con los expertos idóneos para atender incidentes o eventos de seguridad de la información con base en el SGSI de USPEC.
- ✓ **Licenciamiento:** Todas las aplicaciones y servicios prestados por el proveedor deben contar con el licenciamiento acorde con el marco legal y regulaciones que apliquen a USPEC.

6.6 Requerimientos de Seguridad de la Información de la Empresa Proveedora

USPEC exigirá condiciones mínimas respecto a seguridad de la Información para las empresas proveedoras con las que se dé intercambio de información catalogada en los niveles 4, 5 y 6 de Confidencialidad y 5 y 6 de Integridad (Ver **Manual clasificación activos A3-MA-02**).

1. Contar con un Sistema de Gestión de Seguridad de la Información.
2. Presentar la política de Seguridad de la Información referente al servicio o producto que se está prestando a USPEC.
3. Presentar el soporte para el procedimiento de tratamiento de los incidentes de seguridad de la información que puedan darse en el desarrollo del servicio o el producto entregado.

6.7 Requerimientos de Seguridad de la Información de personas Naturales como proveedores

Las personas que actúen como proveedores de USPEC, deberán seguir las Políticas de Seguridad de la Información, definidas para los funcionarios, teniendo como única excepción lo relacionado con el proceso disciplinario, en este caso hará alusión a un incumplimiento de contrato.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
01	30/08/2016	Todos	Se crea el documento

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma: Original Firmado	Firma: Original Firmado Firma: Original Firmado Firma: Original Firmado Firma: Original Firmado	Firma: Original Firmado
Nombre: Fernando Aguilera	Nombre: Jorge Alirio Mancera Cortes Diana Lucia Pinilla Marín Fernando Arturo Vargas Mayra Alexandra Agudelo Carvajal	Nombre: Maria Cristina Palau Salazar
Cargo: Consultor Externo - Globaltek Security SAS	Cargo: Director Gestión Contractual Jefe Oficina de Tecnología Técnico Operativo Profesional Especializado	Cargo: Directora General
Dependencia: NA	Dependencia: Dirección Gestión Contractual Oficina de Tecnología	Dependencia: Dirección General