V SEMINARIO INTERNACIONAL

Quito DISTRITO METROPOLITANO

Archivos: Auditoría a la Gestión Documental y Archivística

Los archivos públicos como activos de información

Alcaldía Metropolitana

Título diapositiva

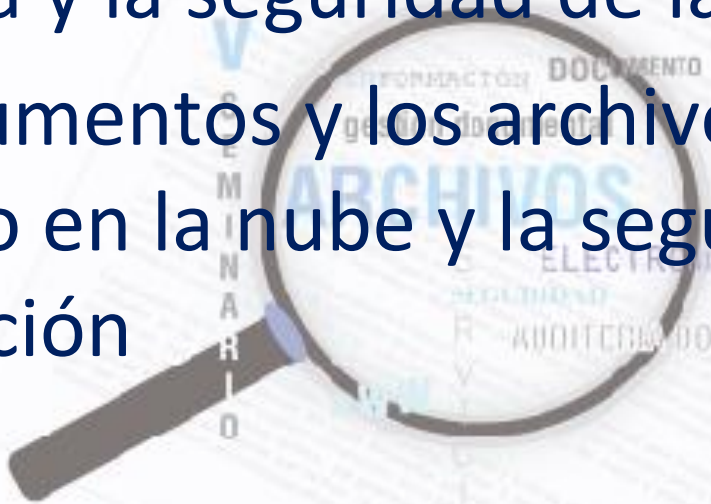
Auditoría documental y seguridad de la información: ¿Como generar un Sistema de Seguridad de la Información?

Alicia Barnard Amozorrutia

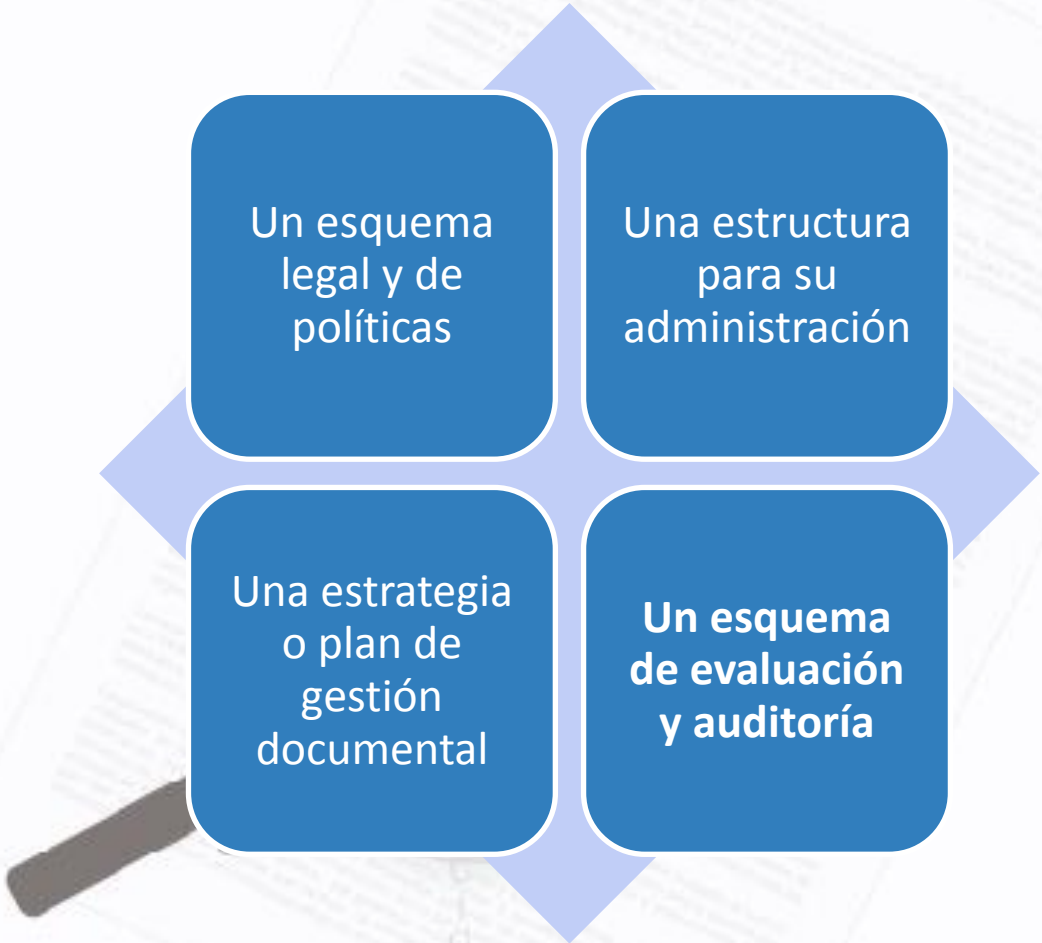
Quito, Ecuador, abril 25, 2014

Contenido

- Auditoría y seguridad de la información. Definición de conceptos
- Gestión de riesgos como herramienta para la auditoría y la seguridad de la información
- Los documentos y los archivos en ambientes de cómputo en la nube y la seguridad de la información



Marco de la Gestión Documental



Gestión documental-ISO 30300

Propósitos (entre otros)

- Proporcionar protección y sustento en litigios incluyendo la **gestión de riesgos** asociados con la existencia o falta de evidencia de la actividad organizacional
- Proteger a los intereses de la organización, los derechos de sus empleados, clientes e interesados presentes y futuros

Sistemas de gestión documental **seguros**

- Mediante el empleo de medidas de control que previenen acciones no autorizadas (acceso, destrucción, alteración , remoción) para respaldar la rendición de cuentas y **la gestión de riesgos**

El proceso de aproximación a un sistema de gestión documental enfatiza la importancia de implementar y operar controles para **manejar los riesgos** en relación con los documentos de archivo dentro del contexto de todos sus riesgos de la organización

Auditoría en la gestión documental

Autoevaluación, evaluación interna o por un tercero para verificar el cumplimiento de políticas o estándares o procesos, establecidos para un sistema de gestión documental mismas que por general concluyen con recomendaciones para cambios en controles y procedimientos útiles a la mejora continua o ajuste de actividades conducentes al cumplimiento dela política para la gestión documental.

La **gestión de riesgos** es una herramienta importante para la auditoría ya que los controles por lo general se establecen para prevenir o reducir riesgos, esto implica que la evaluación de controles identifique los riesgos a prevenir, detectar o corregir.

Seguridad de la información

Teoría y práctica para defender los datos o sistemas de información en contra de acceso no autorizado, destrucción, disrupción, alteración. Lo anterior con el propósito de mantener:

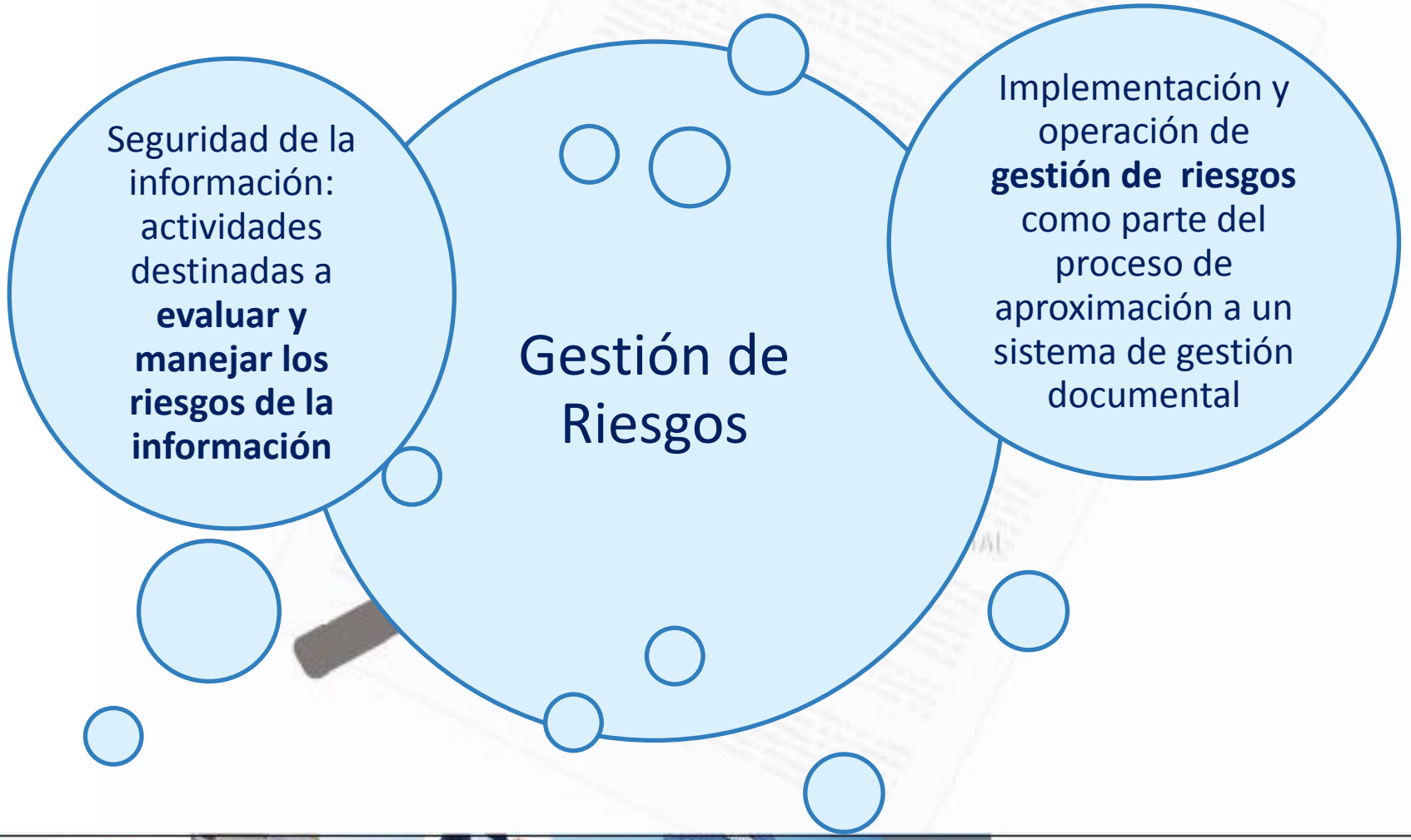
Confidencialidad. Protección de la información de acceso o divulgación no autorizado

La **integridad** a fin de que la **Autenticidad, precisión y completitud** de la información y los métodos de procesamiento no pueda ser modificada sin autorización o que tales modificaciones no pasarán sin ser detectadas.

La **disponibilidad** para asegurar que la información y los servicios asociados estén disponibles a usuarios autorizados que la soliciten en el momento que así la requieran

Política de Información

- Asegurar la compatibilidad con la legislación, regulación o lineamientos aplicables
- Cumplir requisitos de confidencialidad, integridad y disponibilidad de los usuarios de la organización.
- Establecer controles para proteger la información y los sistemas de información en contra de robo, abuso u otras formas de daño y pérdida.
- Motivar para mantener la responsabilidad de propiedad y conocimiento acerca de la seguridad de la información a fin de minimizar el riesgo de los incidentes de seguridad.
- Asegurar que la organización tiene capacidad para continuar sus servicios aun si se presentan incidentes mayores,
- Asegurar la protección de datos personales (privacidad)
- Asegurar la disponibilidad y fiabilidad de la infraestructura de red y los servicios proporcionados y operados por la organización.
- Cumplir con métodos de estándares internacionales para la seguridad de la información. e.g. ISO/IEC 27001.
- Asegurar que los proveedores de servicios externos cumplen con las necesidades y requisitos de seguridad de la información de la organización.


Seguridad de la información: actividades destinadas a **evaluar y manejar los riesgos de la información**
Gestión de Riesgos
Implementación y operación de **gestión de riesgos** como parte del proceso de aproximación a un sistema de gestión documental

Gestión de Riesgos

Proceso de identificar vulnerabilidades y amenazas a los recursos de información utilizados por una organización para alcanzar sus objetivos y decidir cuales controles, si alguno, deben aplicar para reducir el riesgo a un nivel aceptable, basado en el valor del recurso de información de la organización

Etapas de la Gestión de Riesgos

Evaluación del riesgo. Identificar amenazas y vulnerabilidades, describir el riesgo probabilidad de impacto, controles existentes, calificar el nivel de riegos.

Evaluación de mitigaciones. Tomar en consideración los controles existentes para mitigar riesgos identificados.

Implementación de salvaguardas. Establecer medidas de prevención y mitigación de riesgos adicionales a los activos.

Asignación de nivel de prioridad, orden de importancia y orden de actividades para su protección.

Establecimiento de planes tácticos para implementación de controles

Decisión sobre los activos, aceptar riesgos, reducir riesgos, evitar riesgos, transferir riesgos.

Algunas medidas preventivas para control de riesgos

La información de datos personales o sensibles no debería almacenarse en aparatos móviles o en computadoras personales.

Las medidas de seguridad deberían contar con salvaguardas específicas respecto de los documentos de archivo digitales almacenados en computadoras en red que pueden ser accesibles y dañados fácilmente por usuarios remotos.

El acceso a documentos de archivo sensible y su software asociado debería estar controlado por códigos de usuarios o números de identificación.

El acceso a estaciones de cómputo debe estar restringido a empleados autorizados. Las computadoras deberían estar apagadas cuando no están en uso y contar con clave de acceso.

El sistema de software debería terminar automáticamente una sesión de computadora después de un periodo de inactividad.

Las aplicaciones críticas y los documentos de archivo deberían estar aisladas de computadoras accesibles al público dentro de las organizaciones y sin conexión a internet.

Requisitos básicos para los documentos de archivo digitales para verificación de repositorios digitales

- Misión y compromiso para el mantenimiento del objeto digital
- Aptitud organizacional
- Legitimidad legal y normativa
- Políticas eficientes y efectivas
- Infraestructura técnica adecuada
- Adquisición e ingreso
- Preservación del la integridad, autenticidad y uso del objeto digital

¿Y la seguridad de la información en la nube?

Generación X (nacidos en la década de los 70's del siglo pasado)	Generación Y (nacidos a partir de 1980)
Valores	**Valores**
Acceso abierto	Integración de lo público y lo privado, *produsers*
Privacidad/confidencialidad	Fuentes de muchos (*crowdsourcing*)
Derechos intelectuales	Copropiedad
Responsabilidad	Compartir
Compatibilidad	Trabajo en caza (fuerza de trabajo distribuida)
Rendición de cuentas	Trae tu dispositivo al trabajo (utiliza múltiples nubes
Evidencia textual	Convergencia de medios
Memoria registrada	Conectividad constante
Preservación permanente	Lenguaje visual
	Impacto instantáneo, efímero

L. Duranti, 2014

Los retos cuando la información ya no está en un sistema de gestión documental en servidores de la organización

La práctica del re-uso

- Cambios sustanciales en el contexto de materiales.
- Re-uso, modificación, nuevos propósitos

Un campo moral y ético complejo.

- Perfiles, citas, compras compartidos en medios sociales.
- Vigilancia del propio usuario y de sus eventos.
- Autoconocimiento a través de números número de individuos

Se comparte en grupos

- Movimiento de información de un círculo a otro, cruzando líneas de lo publico y lo privado
- Grupos empleados crean material inter-vinculado en relación con un proyecto, interés común sin establecer a quien pertenece el material.
- Las vidas, actividades o iniciativas digitales se vinculan unas a otros.

L. Duranti, 2014

Los retos cuando la información ya no está en un sistema de gestión documental en servidores de la organización

Datos personales mantenidas y controladas por organizaciones privadas y gobiernos.

- Expedientes clínicos (secuencia de genes, medicamentos información sobre seguros) en la nube
- Biografías y datos biográficos están disponibles en la red aunque pertenecen a la plataforma privada que los hospeda.

Gobierno y redes sociales.

- Servicios al ciudadano
- Acceso a la información
- Involucramiento directo de la comunidad

Documentos de archivo en medios sociales

- El publico involucrado en la toma de decisiones de gobierno
- Consultas públicas y propuestas de desarrollo por parte del público
- Anuncios de gobierno
- Medios sociales como medios de comunicación en emergencias

InterPARES Trust

Generar esquemas teóricos y metodológicos que sustenten el desarrollo de redes de políticas, procedimientos, regulaciones, normas y legislación relacionada con los documentos de archivo que son confiados a la internet con el fin de asegurar la confianza pública basada en evidencia de una buena gobernanza, una economía digital fuerte y la memoria digital persistente.

InterPARES Trust. Dominios de Investigación

Infraestructura	Tipos de nube, tipos de contratación, costos, etc.
Control	Metadatos de integridad, cadena de custodia, retención y disposición, control intelectual, etc.
Acceso	Datos abiertos, gobierno abierto, transparencia, derecho a recordar vs. derecho a olvidar
Legislación	Derechos intelectuales, peso de evidencia, autenticación, certificación, cadena de evidencia

Dominios Transversales

Terminología Recursos Políticas Temas sociales Educación

Conclusiones

Hacer uso de la gestión de riesgos como herramienta para la auditoría y los esquemas de seguridad de la información.

Realizar estudios y alianzas para el desarrollo de prácticas y herramientas necesarias para la producción, manejo y preservación de los documentos de archivo auténticos, fiables y accesibles en la nube.

¡MUCHAS GRACIAS!

Alicia

barnard.alicia2@gmail.com