FORTALECIMIENTO EN LA PLATAFORMA TECNOLÓGICA PARA LA MITIGACIÓN DE RIESGO EN UNA COMPAÑÍA ESTATAL

Castro Paez, Diego Armando.
ingenierolinux@hotmail.com
Universidad Piloto de Colombia

***Abstract*:** This document aims to propose a set of building activities that help mitigate the risk to a state enterprise designing management processes, updates, malware and assurance.

***Key words*:** Risk Management, Vulnerabilities, Security Templates, Availability, Confidentiality, Integrity, Malicious Software.

***Resumen*:** El presente documento tiene como propósito plantear en una organización del estado un conjunto de actividades de gestión de aseguramiento de activos con el fin de mitigar los riesgos a los que podría estar expuesta en un mundo tecnológico que cada día descubre nuevos mecanismos de ataque.

I. INTRODUCCIÓN

En la actualidad el campo de la seguridad informática ha venido tomando mucha fuerza e importancia en las organizaciones al punto de destinar recursos en sus presupuestos para proteger sus activos identificados en las organizaciones. Este artículo pretende exponer las estrategias de fortalecimiento para la mitigación de riesgo en la organización. De igual manera esta lectura pretende hacer un compendio de buenas prácticas y dar las pautas de integrar algunos procesos en la organización para fortalecer su riesgo a incidentes de seguridad. También pretende postular tres (3) procesos de gran importancia en la organización para manejo y gestión del aseguramiento, parcheo y defensa contra malware. De este modo y basándose en los procesos actuales de la compañía del estado de la que hablaremos en este artículo. Es de vital importancia fortalecer sus procesos y activos de la compañía por medio de controles que permitan mitigar los riesgos ya que esta compañía al ser del estado tiene contratados un 80% sus servicios tecnológicos.

II. ANTECEDENTES

La compañía que será expuesta en el presente artículo es una compañía del estado del ámbito pensional en donde se describirán las estrategias de fortalecimiento encaminadas a establecer procesos y buenas prácticas a los procesos propios de la compañía.

La situación actual de la compañía la ubica como una administradora de fondos pensionales del gobierno organizada como entidad financiera de carácter especial. Esta empresa nace ante la necesidad de liquidar su predecesora lo cual deja aplicaciones heredadas que continúan soportando la operación de la organización.

III. SITUACIÓN ACTUAL

A. Vicepresidencia De Operaciones y Tecnología

La vicepresidencia de operaciones y tecnología de esta empresa es la que soporta el negocio segregadas en diferentes gerencias. Esto lleva a que las funciones del negocio estén organizadas y orquestadas para dar un servicio.

1) Necesidades actuales: La vicepresidencia de operaciones y tecnología en la actualidad tiene una serie de necesidades para mitigar el riesgo por lo que ha empezado una estrategia de fortalecimiento que ayude a mitigar el riesgo del negocio lo cual se define en las siguientes actividades:

- Apoyar los proyectos en curso orientados a fortalecer el aseguramiento en la plataforma tecnológica (vulnerabilidades y aseguramiento)
- Apoyar la actualización de las matrices de roles empresariales.
- Revisión de requisitos de seguridad y registros de auditoría de los sistemas de información de la compañía.

2) Tercerización: Una característica de una compañía del estado es tercerizar sus servicios corporativos por medio de casas de software o proveedores fabricantes de soluciones tecnológicas. Esta compañía tiene contratos con proveedores muy reconocidos en la industria de tecnología los cuales tienen un estándar y metodologías pero en algunos escenarios guías dispersas en el momento de efectuar entregables.

3) Riesgo en la organización: El riesgo en esta administradora de fondos pensionales conlleva a la posibilidad de que una amenaza se produzca sobre alguno de sus activos dando lugar a un ataque en la organización que pueda poner afectar el core del negocio. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte [1] de la amenaza de un tercero con el objetivo de obtener algún beneficio económico o simplemente sabotaje empresarial.

4) Amenazas en la organización: Como sabemos una amenaza a un sistema informático "es una circunstancia que tiene el potencial de causar un daño o una pérdida". Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Como ejemplos de amenaza están los ataques por parte de personas al igual que los desastres naturales que puedan afectar a esta compañía [2]. También se pueden considerar amenazas los fallos cometidos por los usuarios o administradores del sistema o los fallos internos tanto del hardware o cómo del software en sus centros de datos o aplicativos que soportan la operación.

5) Vulnerabilidades en la organización: En esta compañía no es la excepción en tener debilidades en sus sistemas que pueden ser utilizadas para causar un daño [3]. Las debilidades pueden aparecer en los componentes de una la plataforma tecnológica tanto en el hardware, software e incluso personas.

IV. ACTIVIDADES DE FORTALECIMIENTO

A. Apoyar los proyectos en curso orientados a fortalecer el aseguramiento en la plataforma tecnológica (vulnerabilidades y aseguramiento)

Para atender este frente de necesidad es indispensable aplicar una metodología o guía para efectuar análisis de vulnerabilidades basados en pruebas usando herramientas como escáneres y su remediación haciendo planes de gestión de vulnerabilidades. Esta organización en su área de seguridad informática diseñó dos esquemas de gestión de vulnerabilidades las cuales son:

1) Análisis de vulnerabilidades programado: Este tipo de análisis consiste en hacer un inventario de activos en la compañía y efectuar un cronograma periódico trimestral con un plan de disponibilidad de pruebas de caja blanca y caja gris.

2) Análisis de vulnerabilidades por demanda: La organización debe establecer un procedimiento de solicitud que permita estandarizar el proceso e implantarlo en los procesos de pruebas y certificación de un desarrollo a producción con el fin de contemplar desde el desarrollo la seguridad

en las liberaciones de entregables y de este modo tomar acciones preventivas y no reactivas.

3) Administrar servicios de terceros: En los requerimientos desarrollados por terceros es de suma importancia vincular buenas prácticas de desarrollo y estándares que sean concebidas con un enfoque no sólo de funcionalidad sino de seguridad.

4) Análisis y seguimiento del plan remediación de vulnerabilidades: Este proceso ha de darle trazabilidad a las vulnerabilidades encontradas en la organización y es un paso primordial que ayuda a establecer un plan de acción y establecer mejoras en los activos con vulnerabilidades. Esto se debe hacer clasificando las vulnerabilidades como crítica, alta, media, baja e informacional que son las informadas por la mayoría de herramientas de vulnerabilidades del mercado y estableciendo un acuerdo de nivel de servicio o también llamados ANS. Dichos acuerdos servirán para determinar actividades puntuales a la hora de efectuar el plan de remediación. La organización deberá dejar como política que las vulnerabilidades catalogadas como críticas, altas y medias deben ser corregidas lo más pronto posible. Las catalogadas como bajas e informacionales deben ajustarse en el mediano plazo y tomarse en cuenta las recomendaciones sugeridas por el área de seguridad informática dentro de la organización.

5) Gestionar boletines y alertas de los fabricantes de los activos de TI: La organización debe estar al tanto de nuevas vulnerabilidades que se detectan día a día en el mundo. Por lo tanto debe suscribirse a boletines diarios, semanales o periódicos que le den a conocer nuevos riesgos a los que están expuestos los activos de la compañía. Para tratamiento de estos riesgos una buena recomendación es suscribirse a uno de los más importantes portales que publican a diario vulnerabilidades como lo es Hispasec el cual lleva desde el año 2000 brindando servicios de seguridad en tecnología junto con otros portales que brindan información relevante del estado de tecnologías del medio. En resumen son un servicio de noticias y análisis sobre seguridad informática.

6) Gestionar la aplicación de plantillas de seguridad: Para entender este dominio del artículo es indispensable definir ¿qué es una plantilla de seguridad? Por esto es necesario definirlo como el documento físico o digital con un conjunto de configuraciones y parametrizaciones que fortalecerán la seguridad de un activo en la compañía. En toda organización es de vital importancia implantar en sus activos la definición de plantilla de seguridad con el fin de asegurar alinearse a las políticas de endurecimiento mitigando el riesgo de vulnerabilidades que vienen con la configuración predeterminada de un sistema o también configuraciones no apropiadas por parte de los administradores de dichos sistemas.

Por lo anterior aclarado la organización debe establecer un proceso de gestión de plantillas de seguridad sobre los activos estableciendo métricas de gestión y además los acuerdos de nivel de servicio también llamados ANS que oficialicen el proceso dentro de la compañía. Por tanto un flujo de gestión de plantillas (ver figura 1) de seguridad generará una aplicación de aseguramiento de activos llevando traza de la gestión y asignando responsables de las actividades.

A este proceso se deben involucrar a los gestores de cambio, dueños de dominio y grupos de seguridad. En donde sus funciones deberán dar valor al proceso.

A continuación se presenta una propuesta de proceso como opción a la gestión de plantillas de seguridad. Cabe aclarar que este proceso se está contemplando a una organización que ha venido afinando sus áreas y con ellos sus procesos.

Nota: Los diagramas propuestos en este documento han sido elaborados en la herramienta Bizagi Modeler con el fin de ver de una manera gráfica el flujo del procesos que se plantean como implementación de la organización gubernamental expuesta en este documento.

a) Grupos de Seguridad

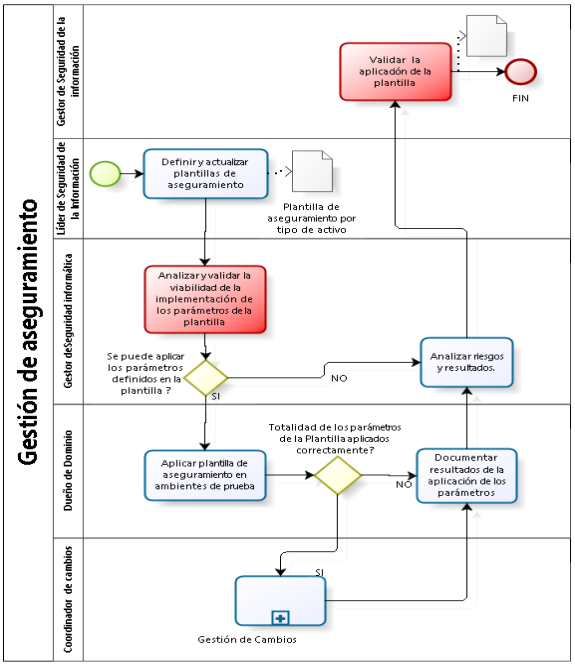
i. Definir y elaborar plantilla de seguridad.
ii. Validar la aplicación de la plantilla.
iii. Documentar el análisis de riesgos y resultados.

b) Dueños de dominio

i. Definir la aplicabilidad de la plantilla.
ii. Aplicar la plantilla.

c) Gestor de Cambios

Figura 1.



Fuente: Autor.

7) Gestión de Software Malicioso: El control de software malicioso sobre los activos de la compañía es muy importante en la ya que determina la disminución de riesgo al que se enfrenta cualquier compañía al estar expuesta a amenazas que puedan comprometer la integridad, confidencialidad o disponibilidad de la información por medio de software diseñado para infiltrarse y alojarse con el objetivo de dañar, alterar información, retrasar procesos o hacer puertas traseras que permiten hacer fuga de información que para este caso en la compañía al ser financiera y al manejar información de alta criticidad debe tener estipulado en sus procesos la gestión de riesgos al software malicioso. Por eso desde la solicitud de instalación de herramientas antivirus y centralización de consola de dicha herramientas deben permitir un manejo adecuado de los posibles eventos que se puedan materializarse en cuanto a malware se refiere.

Como en el dominio anterior este proceso también se deben involucrar a gestores de cambios, dueños de dominio en este caso infraestructura y a los grupos de seguridad informática (ver figura 2).

a) Grupos de seguridad

i. Solicitar instalación de antivirus en los activos de la compañía.
ii. Revisar las consolas de antivirus y evaluar regularmente sobre los riesgos de nuevas posibles amenazas.
iii. Elaborar informes de evaluación de riesgos y amenazas.
iv. Elaborar planes de acción para remediar amenazas.

b) Dueños de dominio

i. Instalar y activar herramientas de antivirus en los activos tecnológicos de los ambientes productivos como no productivos.
ii. Medir la efectividad de la operación del antivirus llevando control de los eventos reportados por la herramienta.
iii. Distribuir todo el software de protección de una forma centralizada

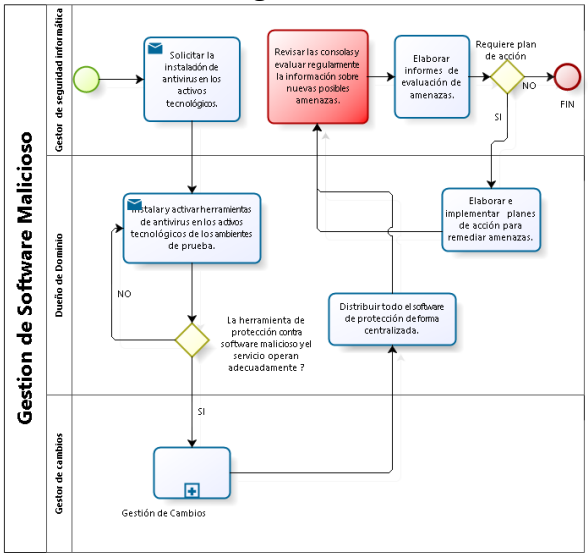
c) Gestor de cambios

i. Gestionar y controlar los cambios efectuados sobre los activos de la organización.

A continuación se presenta una propuesta de proceso como opción a la gestión de software malicioso. Cabe aclarar que este proceso se está contemplando a una organización que ha venido afinando sus áreas y con ellos sus procesos.

Se incluyen en algunos pasos la generación de informes en ciertas actividades específicas ya que son el insumo para la gestión y planes que se tengan que efectuar en la compañía. Además la gestión de software malicioso debe también tener una estrategia para un escenario de la compañía en donde los funcionarios comerciales están dispersos por todo el país con el equipo portátil asignado lo que dificulta un despliegue de configuración de plantillas de seguridad.

Figura 2.



Fuente: Autor.

8) Gestión de Parches: La definición más resumida de un parche es "*códigos que corrigen errores de seguridad de los sistemas"* [4] pero en la actualidad no solo se hacen a los sistemas sino a las aplicaciones de la organización. Por eso es de vital importancia que la compañía adopte y defina una política de parchado sobre los activos en general. Estas actividades van en sincronía con las actualizaciones que los proveedores liberan parches de actualización y la organización está destinada a gestionar la instalación del mismo (ver figura 3).

a) Grupos de Seguridad

i. Adquirir el parche
ii. Evaluar el impacto del parche en el sistema.
iii. Establecer repositorio de parches implementados.

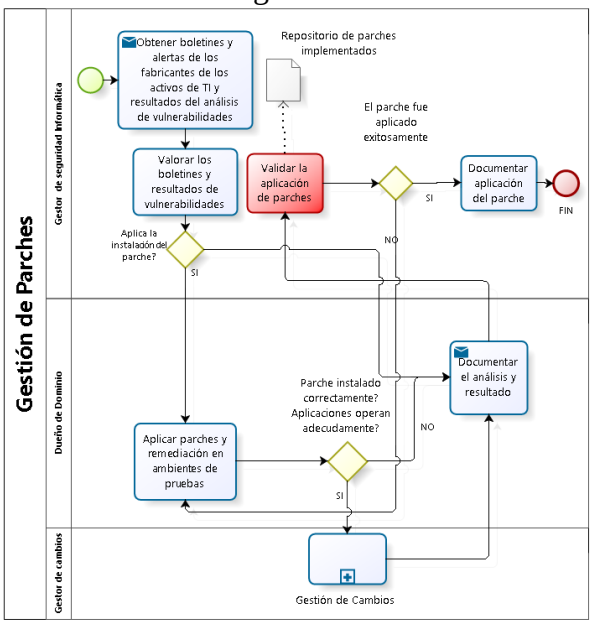
b) Dueños de dominio

i. Aplicar parches y remediación en ambientes de pruebas.
ii. Verificación de parches instalados correctamente y verificación de normalidad del funcionamiento del activo.

c) Gestor de cambios

i. Gestionar la ventana de tiempo para la instalación de parches.

Figura 3.



Fuente: Autor.

9) Gestión de cuentas privilegiadas: El control de cuentas privilegiadas en la

compañía del estado es un punto clave en la seguridad el cual debe tener una trazabilidad y un control. Para esto las acciones para fortalecer la seguridad y mitigar los riesgos que pueden existir. Por eso la organización debe establecer un manual de administración de credenciales privilegiadas así como incorporar una herramienta que pueda automatizar el control de utilización de cuentas privilegiadas ya que en la actualidad en esta organización son cuentas que se comparten entre los administradores de los activos y lo único que hay oficial en algunos casos que se han podido identificar son la firma de cartas de riesgos por el uso compartido del password de este tipo de usuarios. Hay herramientas por ejemplo User Administration Tool for IBM® Rational® ClearQuest® [5] que permiten de una manera tener una cuenta privilegiada haciendo que pueda ser utilizada por múltiples usuarios asignando al usuario solicitante un password temporal enviado a su correo corporativo llevando traza de su utilización por sesión. Tipos de herramientas así ayudan a tener alertas de riesgo asociado a cuentas privilegiadas que en manos equivocadas y al no llevar traza de su uso pueden llegar a impactar a la organización en escenarios de empleados descontentos o no autorizados que quieran obtener un beneficio económico o simplemente de sabotaje empresarial.

10) Verificación de cumplimiento de requisitos de seguridad: Al ser una compañía del estado la expuesta en este artículo es de aclarar que sus procesos están en su gran mayoría tercerizados por lo que sus convocatorias son públicas. Esta compañía ha mitigado el riesgo de seguridad aplicando ítems de seguridad en sus licitaciones. A continuación se presentan conceptos básicos que la organización deberá incluir en sus contrataciones con los terceros que le brinden un servicio o producto.

11) Conectividad en línea con el sistema transaccional: Esta compañía tiene una modalidad de la manera que sus clientes hacen sus aportes por lo que debe contarse con un sistema transaccional (ST) que se encarga de gestionar el enrutamiento, procesamiento, validación y autorización de las transacciones con las redes de recaudo. Por ningún motivo se deben permitir operaciones fuera de línea con el sistema transaccional. Por lo tanto debe contar con un mecanismo alterno que garantice conectividad con el ST en caso de contingencia.

12) Cifrado de archivos red de recaudo con el sistema transaccional: Esta compañía maneja envió de archivos con información de recaudos y por tal motivo los archivos que se intercambien entre la red de recaudo y el sistema transaccional deberán viajar cifrados desde la fuente utilizando el sistema transaccional pretty good privacy (PGP) con un tamaño de llave de mínimo 1024 bits. Lo anterior brinda el servicio de confidencialidad en la información de los archivos planos que se manejan entre la red de recaudos y la compañía de pensiones.

13) Seguridad de la información: Es de gran importancia que el proveedor este alineado con el estándar NTC-ISO-IEC 27001:2013 el cual contiene los requisitos del sistema de gestión de seguridad de la información. Esto ayuda a mitigar el riego tercerizado dando lineamientos en materia de seguridad de la información.

14) Seguridad en conectividad y comunicaciones: La comunicación entre los recursos de la red de recaudo y el sistema transaccional de la compañía estatal debe realizarse a través de un dispositivo de seguridad perimetral en un esquema de alta disponibilidad (firewall, ips, etc.) y garantizar que entre recursos de la misma empresa se apliquen esquemas de seguridad perimetral acorde a la sensibilidad de la operación e información. La administración, gestión, soporte y monitoreo de las plataformas debe realizarse a través de

conexiones seguras (VPN/SSL, canales dedicados).

15) Log auditoría: Es muy importante la trazabilidad en la información y mucho más cuando son datos financieros por tanto el proveedor debe generar y mantener un log transaccional o de auditoría para registrar las operaciones realizadas en los puntos de recaudo que permita evidenciar los accesos a la información transaccional de esta compañía del gobierno. El tercero siempre deberá proporcionar la información registrada en el momento en que esta compañía estatal la requiera en el formato y estructura llevando consigo siempre unas buenas prácticas de registro de logs. Una propuesta de una plantilla básica para un check para revisión de logs debe contener los siguientes ítems basándose en el ¿qué? ¿Cómo? ¿Cuándo? ¿En qué contexto? han sucedido los eventos de los sistemas [6].

Ítems

i. ¿El log indica qué evento o acción ha ocurrido?
ii. ¿El log detalla qué entidades (clases, tablas) han estado involucradas?
iii. Si hay un cambio de estado, el log contiene ¿cuál era el estado anterior? ¿cuál es el estado nuevo?
iv. ¿El log indica el punto del código ha ocurrido el error? Es decir componente, clase, fichero de código, método o bloque de ejecución, línea de código.
v. ¿Registra la hora, minuto y segundo del evento?
vi. ¿Genera una traza secuencial o causal?
vii. ¿Registra estados o variables: propios de la ejecución (parámetros) de personalización o específicos de usuario, referentes a la sesión o transacción en ejecución?
viii. ¿Indica transacciones o peticiones relacionadas cuando estemos en entornos concurrentes?
ix. ¿Indica el usuario conectado en la base de datos que realizó el cambio?
x. ¿Se depura la información de logs?

16) Políticas de backup: Los proveedores siempre debe contar con políticas de backup, restauración y retención de la información del servicio transaccional prestado a esta compañía del gobierno para mitigar el riesgo de no tener disponible la información cuando se requiera además durante la vigencia del contrato que se haga con el prestador del servicio siempre se debe estar garantizando la recuperación completa de la información transaccional realizada. Todo lo anterior basándose en buenas prácticas en las políticas de backups "*La política de backups es la definición de los diferentes aspectos de las copias de seguridad: ¿De qué se debe hacer backup? ¿Cada cuánto se realiza la copia de seguridad? ¿Qué retención deben tener? ¿Dónde se guardan las copias? ¿Cuánto tiempo es aceptable que se pueda tardar en recuperar datos?"* [7].

17) Capacidad de manejo de concurrencia transaccional: El proveedor debe garantizar el 100% de atención de las transacciones, mediante el manejo adecuado de transacciones concurrentes, altos volúmenes transaccionales, manejo de colas transaccionales entre otros aspectos a considerar en la operación. Lo anterior con el fin de mitigar el riesgo de indisponibilidad lo cual impacta el core del negocio de forma drástica. A esto en sus licitaciones deben exigirse pruebas de concurrencia y de estrés que permitan garantizar que el sistema pueda soportar alta transaccionabilidad.

18) Actualización de software

La actualización de software relacionada con la prestación del servicio con la infraestructura de esta empresa a quien le definimos las actividades de fortalecimiento para la mitigación de riesgo deberá ser manejada con metodología de atención de requerimientos y será liberada en producción mediante proceso de control de cambios.

V. CONCLUSIONES

Las buenas prácticas de seguridad en el campo corporativo son importantes para la mitigación de riesgo que se pueden presentar en la organización donde no se toman medidas y controles que garanticen la confidencialidad, integridad y disponibilidad de los activos en la compañía. Este artículo plantea el proceso que debe implantarse y quedar como política los procesos de gestión de parches aseguramiento y software malicioso como los procesos más útiles y otros procesos no menos importantes que ayudan a la gestión de la seguridad en la organización. Es de vital importancia que la organización acoja estos procesos y los convierta en políticas desde la alta gerencia para que tengan todo el respaldo corporativo de tal forma sea de gran relevancia en la compañía. El riesgo siempre estará latente pero ante políticas de gestión de seguridad que se implanten puede ayudar a mitigar este riesgo que se puede materializar en eventos catastróficos por no haberse efectuado una gestión de riesgo.

Esta compañía cada vez irá madurando en sus procesos mediante la capacidad que tenga de blindar sus procesos y activos. Entregando valor en cada aplicación de políticas y controles que hacen toda la línea de negocio. Además es de aclarar que esta compañía lleva menos de 5 años en operación en donde ha logrado muchos retos de operación de su predecesora. Todo lo anterior se ha logrado por medio de una alineación del negocio con tecnología y dando gran valor al aspecto de seguridad en la organización que cada día mejora sus procesos de aseguramiento dando tranquilidad el negocio.

REFERENCIAS

[1] [2] [3] Codejobs, Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?, Global Solutions Directory,Available: https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

[4] Purificación Aguilera López, Seguridad informática, Informatica y Telecomunicaciones, Editorial Editex.

[5] IBM, User Administration Tool for IBM® Rational® ClearQuest® Web version 1.1, Global Solutions Directory,Available: http://www-304.ibm.com/partnerworld/gsd/solutiondetails.do?solution=48570&lc=en&stateCd=P&tab=2

[6] Bytes & Chips, Consejos y buenas prácticas del logging de aplicaciones, Just another technology blog, Directory,Available: https://bytesandchips.net/2012/10/02/consejos-y-buenas-practicas-del-logging-de-aplicaciones/

[7] Capside, Backups 101: ¿Qué debemos tener en cuenta? Políticas, retención, storage, restauración y herramientas. Alba Ferrer | SysOps Team Manager, Directory,Available: https://bytesandchips.net/2012/10/02/consejos-y-buenas-practicas-del-logging-de-aplicaciones/