

RECOMENDACIONES PARA SOFTWARE E INFRAESTRUCTURA SEGURA

Rodrigo Ferrer CISSP
rodrigo.ferrer@sisteseg.com
Bogotá
Colombia
www.sisteseg.com

El objetivo primordial de la elaboración de este documento, se relaciona con las mejores prácticas de seguridad que se deben tener con relación al software para lograr la integridad, la confidencialidad y la disponibilidad de la información. Por otro lado, la protección y el buen uso de los activos de información deben estar dentro de un marco conceptual y lineamientos en seguridad, que permitan la mejora gradual en la seguridad de la información, sin afectar la operación de la compañía y sin disminuir la productividad hasta ahora alcanzada por las empresas. También es importante que se consideren los costos, beneficios e implicaciones asociados a cualquier tecnología o nuevo proceso a implantar de acuerdo a los lineamientos en seguridad de la información adoptados por las empresas.

Para lograr lo anteriormente expuesto como objetivo de este estudio, este documento establece los lineamientos que los sistemas deben seguir para proteger adecuadamente la información que el procesa o almacena, de acuerdo a estándares internacionales que han sido probados en grandes e importantes empresas a nivel mundial.

A continuación recomendaciones en la red:

- ❖ Firewall
 - Tecnología de packet filtering (filtrado de paquetes)
 - Tecnologías stateful (comprobación de estado de conexión)
 - DPI (Deep Packet Inspection-inspección profunda de los paquetes)
 - Firewall de nivel de aplicación (proxy)
- ❖ IDS (sistemas de detección de intrusos)
 - Gestión adecuada de los reportes e informes
- ❖ IPS (sistemas de prevención contra intrusos)
- ❖ Switches de Core
 - Switch fabric redundante (recomendado)
 - Fuentes de poder redundantes
 - Soporte de nivel 3 (protocolo IP y listas de control de acceso-ACL)
- ❖ Switches de piso
 - Control de acceso lógico por dirección MAC
 - Listas de control de acceso (ACL)
- ❖ Servidores
 - Sistema operativo asegurado (Hardening)
 - Fuentes de poder redundante
 - Sistemas de discos duros confiables (Ej. RAID)
- ❖ Infraestructura Física
 - Tecnologías de control de acceso
 - Sistemas biométricos
 - Tarjetas inteligentes
 - 2 o 3 factores de autenticación

- ❖ Enrutadores perimetrales
 - Sistema operativo actualizado periódicamente y por demanda
 - Listas de control de acceso (ACL)
 - Gestión de contraseñas de administración
 - Protocolos de acceso seguro
 - SSL
 - SSH
 - HTTPS
 - IPSEC
 - SNMP V3
- ❖ Antivirus y gateway antivirus
 - Actualizable dinámicamente
 - Amplia base de datos
- ❖ Antispyware
 - Actualizable dinámicamente
 - Amplia base de datos

Entro otros objetivos que se buscan en seguridad de la información se cuenta con:

- **Proteger los sistemas** asegurándose de que se dispone de las tecnologías, personas y procesos adecuados para garantizar que los datos sólo son accesibles a los usuarios fiables y que los sistemas están configurados correctamente y actualizados para ayudar a mantener fuera a los usuarios no autorizados.
- **Detectar las intrusiones frustradas**, las violaciones de seguridad, los comportamientos inesperados y los indicios anteriores a los fallos. Este tipo de detección es como configurar el sistema de alarma de seguridad de su casa para que le avise de los posibles peligros.
- **Defender los sistemas** tomando medidas correctivas automáticas cuando se sospecha o se da una violación de seguridad. La defensa es como llamar a la policía durante un ataque.
- **Recuperar los ordenadores** que han estado en peligro, son sospechosos o han fallado depende de contar con sistemas y procesos adecuados para restaurar una máquina y sus datos al último estado correcto conocido, al tiempo que se minimiza su tiempo de inactividad. En las tecnologías de la información (TI), significa tener sistemas de copia de seguridad que permitan restaurar rápidamente los sistemas infectados a un buen estado previamente conocido.
- **Administrar y coordinar** la protección, detección, defensa y recuperación de los sistemas críticos significa tener las directivas y procedimientos adecuados para coordinar estas actividades. La administración es como fijar unas reglas para la seguridad del hogar, contratar un seguro y actualizar sus directivas conforme cambian sus propiedades y posesiones. Del mismo modo, la administración de seguridad TI requiere que se mantengan actualizadas las directivas de seguridad según cambian las amenazas y los valores con el paso del tiempo. Se pueden automatizar muchas tareas de administración de seguridad y configurar los sistemas para avisar al administrador cuando se detecten violaciones de las directivas de conducta o de rendimiento especificadas para los usuarios. La administración de seguridad se basa en administradores correctamente entrenados en las mejores

prácticas que implementan regularmente los procedimientos y directivas de seguridad.

Así mismo, es importante que las recomendaciones expuestas en este documento vayan de la mano de la recomendación ISO 27001, reflejando así las mejores prácticas en seguridad de la información sobre los activos. A continuación se describen los dominios considerados por la norma, los cuales deben ser acogidos por las empresas, dentro de su proceso de mejora de la seguridad de la información.

Política de seguridad: Existencia de un documento de políticas de seguridad.

El objetivo de optar por el seguimiento a un conjunto de políticas en seguridad de la información, es brindar apoyo y orientación a la dirección y a los empleados con respecto a la seguridad de la información de acuerdo con los requisitos del negocio, los reglamentos y las leyes pertinentes instauradas en la constitución colombiana, para lograr una operación segura y continua del negocio.

Organización de la seguridad: Gestionar la seguridad de la información dentro de la empresa. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros)

Gestión de activos: Se relaciona con el mantenimiento y protección apropiados de todos los activos de información.

Seguridad del Recurso Humano: Este dominio busca asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles a desempeñar minimizando los riesgos relacionados con personal.

Seguridad Física y del entorno: Busca prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones.

Gestión de comunicaciones y operaciones: Se busca asegurar la correcta y segura operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica).

Control de acceso: Se realiza el control físico o lógico de los accesos a los activos de la información, incluyendo por ejemplo acceso físico a los sistemas operativos o aplicaciones. Este dominio es uno de los más importantes desde el punto de vista del sistema, ya que aquí se controla el acceso lógico por parte de los usuarios autorizados a esta aplicación, evitando por lo tanto que usuarios no autorizados llegasen a afectar la disponibilidad, la integridad y la confidencialidad de la información.

Adquisición, desarrollo y mantenimiento de sistemas de información: Asegurar la inclusión de todos los controles de seguridad en los sistemas de información nuevos o en funcionamiento (infraestructura, aplicaciones, servicios, etc.). También regula la adquisición de software para la organización y los contratos de soporte y mantenimiento asociados a ellos.

Hoy en día, Los bienes relacionados a los sistemas de la Información, son cada vez más valorados por las organizaciones, por lo cual, cualquier esfuerzo por mejorar su seguridad genera ganancias y mejoras en la productividad. En específico, las aplicaciones software y sistemas de información, deben comenzar a ser desarrollados, considerando la seguridad como una propiedad fundamental e importante, que no

puede ser considerada al finalizar el ciclo de desarrollo, si no, desde las etapas tempranas, es decir, cuando se plantean los requerimientos funcionales.

La metodología principal en durante este proyecto, consistió en controlar y gestionar principalmente los siguientes aspectos:

A continuación también mencionaremos los principios de desarrollo seguro de software que fueron utilizados en la realización de los programas:

1. Se analizaron la gran mayoría de amenazas que pueden afectar al desarrollo seguro y también se consideraron posibles futuros ataques al sistema como:

- ❖ Buffer Overflow¹, es decir cuando un espacio de memoria pueda ser escrito con más información que la existente en este espacio limitado causando un problema de prestación de servicio o la inclusión de un código malicioso dentro de la ejecución del programa.
- ❖ Código malicioso, puede ser insertado de manera no visible dentro de un proceso de desarrollo, para esto se consideró la protección tanto física como lógica a los ambientes de desarrollo y controles tecnológicos para verificar de manera que continua que el código no sea modificado durante su creación por usuarios no autorizados. También se consideraron técnicas que permiten por medio de una operación matemática calcular un código que nos informa que la integridad del programa ha sido o no afectada. La arquitectura por capas, fundamento de nuestro desarrollo, permite controlar el acceso no autorizado, pues existen componentes que son los únicos que pueden acceder a elementos de la aplicación.
- ❖ Datos no validos a la entrada, la aplicación como tal realiza las verificación con el fin de controlar la información que entra con el fin de evitar que campos inválidos puedan afectar el comportamiento interno del sistema como sus respectivas salidas. La idea es que cualquier tipo de datos entrando al software será verificado con el fin de que no contenga algún tipo de ataque. Los sistemas por su arquitectura y tecnologías de desarrollo facilitará los procesos de mejoras en lo referente al tema de seguridad, dado que las características de los riesgos presentes en los sistemas de información obedecen a un patrón muy dinámico en el tiempo, obligando a los desarrolladores, administradores de la red y oficiales de seguridad estar en un ciclo continuado de aprendizaje de nuevas tecnologías para defenderse con las amenazas tanto externas como internas y también un entendimiento detallado y profundo de las características fundamentales de estas amenazas para estar mejor preparados para enfrentarlas, así como una gestión adecuado de incidentes de seguridad que puedan ocurrir sobre el sistema; documentarlos adecuadamente y en la medida de lo posible aprender de ellos y realizar idóneamente las medidas correctivas necesarias y requeridas.

Por último se debe controlar adecuadamente los datos de entrada a las aplicaciones, considerando los casos de uso con el fin de detectar los siguientes errores:

- Valores fuera de rango

¹ Se puede traducir como desbordamiento de la memoria.

- Caracteres inválidos en los campos de datos
 - Datos incompletos o faltantes
 - Datos Inconsistentes de Control
 - Se debe hacer una revisión periódica de campos importantes de los datos, con el fin de confirmar su validez e integridad
 - Se deben inspeccionar los documentos de entrada para detectar algún cambio no autorizado. (Todos los cambios a los documentos de entrada deben poseer su respectiva autorización del propietario de la información)
 - Se deben tener procedimientos para responder a errores de validación.
 - Se deben tener procedimientos para detectar la veracidad de los datos.
 - Se deben definir las responsabilidades de todo el personal involucrado en procesos de entrada de datos.
- ❖ Errores de procesamiento se pueden evitar haciendo un uso adecuado de los recursos que ofrece el sistema. Por medio de una adecuada gestión entre los llamados a los recursos ofrecidos por el sistema operativo y la verificación de los códigos de errores se controla de manera adecuada el acceso a los recursos de procesamiento.

2. Se debe estudiar también detenidamente quienes puede acceder a la aplicación y a los datos y en qué entorno se va a gestionar, etc. Realizando un análisis de los riesgos de posibles ataques a la aplicación, lo que genere los controles adecuados que se han implementado en el sistema con el fin de mitigar el impacto que pudieran tener estos posibles eventos adversos.

3. Se deben integrar los requisitos de seguridad con todas las etapas del ciclo de desarrollo de software, y no realizar únicamente pruebas al final lo que pudiera reflejarse en riesgos permanente en seguridad de la información y un costo mayor de implantación de los controles respectivos. Por su parte, el *release* arquitectónico validó requerimientos no funcionales, incluyendo la seguridad y buenas prácticas.

4. Es claro hoy en día la importancia de la seguridad en los entornos de desarrollo software. Para considerar esta seguridad nos basamos en estándares como el ISO 17799, o el *Control Objectives for Information and related Technology* (COBIT) cuyo objetivo es organizar y armonizar distintos estándares internacionales, relacionados con la administración de la Tecnología de la Información en las organizaciones. COBIT presenta un conjunto de mejores prácticas, enfocadas en el control más que en la ejecución, que permiten optimizar la inversión en TI que una organización realiza. También se han considerado lineamientos provenientes del *Information Technology Infrastructure Library* (ITIL) el cual ofrece un marco común para todas las actividades del departamento TI, como parte de la provisión de servicios, basado en la infraestructura tecnológica.

Los tres modelos anteriormente presentados, incorporan la seguridad desde distintas perspectivas, algunas de las cuales son similares y otras complementarias. A partir de estas diferencias y similitudes se puede determinar una serie de recomendaciones y mejores prácticas de la seguridad en relación al desarrollo de software.

Los factores a considerar con base en lo anteriormente expuesto están:

- ❖ Factores humanos relacionados con las habilidades y conocimientos que deben poseer los equipos desarrolladores, con el fin de desarrollar un software seguro de acuerdo al sistema de gestión de seguridad.
- ❖ Prácticas organizacionales declaradas e instauradas que deben respetarse y aplicarse, es decir una cierta madurez en el emprendimiento de desarrollos en sistemas.
- ❖ Productos obtenidos y acabados, para cada uno de los cuales se debe realizar una rigurosa validación y verificación, garantizando que cumple con los estándares y requisitos de seguridad declarados en las fases iniciales del proyecto.

Con base en los estándares y metodologías (ISO 17799, COBIT e ITIL) anteriormente estudiadas, consideramos relevante en lo relacionado con el desarrollo de software, los siguientes temas:

- Control sobre el código de software.
- Herramientas de desarrollo de software.
- Prueba & entrenamiento.
- Documentación.
- Metodologías de Control de cambios.
- Separación de ambientes y funciones.
- Controles criptográficos posibles
 - SSL
 - HTTPS
 - IPSEC
- Firmas digitales si fuera necesario

Gestión de incidentes de seguridad: Permitir que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados de tal manera que se tome una acción correctiva adecuada y en el momento indicado. En caso de presentarse un incidente de seguridad, este debe ser comunicado inmediatamente al responsable de ello en la empresa, con el fin de tomar las medidas correctivas tendientes a su solución y además de ellos documentarlos, para que en un futuro se pueda prevenir la ocurrencia de eventos similares. Se debe dar especial énfasis en lo relacionado con el software y crear unos formatos y procedimientos adecuados, que nos indiquen el camino a seguir en caso de presentarse problemas relacionados con la confidencialidad, integridad y disponibilidad del sistema, con el fin de tomar medidas correctivas apropiadas y también medidas preventivas que evite que el mismo problema se vuelva reiterativo.

Gestión de la continuidad del negocio: Enfocado en reaccionar en contra de interrupciones a las actividades de la función misional y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y por otro lado, asegurar que se recuperen a tiempo.

Cumplimiento: Busca prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.