Lineamientos de Seguridad

Versión 1.2

Dirección de Tecnología
Documento XM Lineamientos de Seguridad
Junio, 2016

Control de Cambios

Versión	Fecha	Responsable	Descripción
1.2	2016-06-30	Rubén Villa	Se adiciona una nota en el numeral 3 de Auditorias en cuanto a los logs. Se ajusta el lineamiento en el numeral 3 Auditorias sobre el tiempo de almacenamiento y retención.
1.1	2016-01-26	Rubén Villa	Se ajusta el numeral 1.1 de Generalidades adicionando el responsable y definiciones. Se agrega al numeral 1.2 Criptografía y comunicaciones el tema de soluciones en la nube. Se especifica en el numeral 1.4 Ambientes de pruebas y calidad los tipos de equipos a que se refiere, el responsable. Adicional se define Appliance. En el numeral 2 se agrega definición de correo electrónico por medio de SMTP. En el numeral 3 se ajusta el párrafo de log. En el numeral 4 se especifica sobre la entrega de la información confidencial que no puede ser entregada por temas de regulación. Se especificar en la nota que los controles de seguridad dependen del proyecto a desarrollar.
1.0	23/10/2015	Nataly Zapata Sandro Usuga Rubén Villa	Versión 1.0

Contenido

INTRODUCCION

Este documento contiene la presentación de lineamientos y estándares de seguridad informática para la minimización del riesgo asociado a fallas, problemas e incidentes de seguridad.

1. Seguridad en Sistemas de información

1.1 Generalidades

- Lo sistemas de información deben autenticar y autorizar basados en la arquitectura de referencia y deben utilizar el protocolo LDAP por medio de directorio activo.
- Se debe asegurar el cumplimiento del lineamiento definido para la administración de cuentas de usuario. Ver documento DOT Administración de cuentas de usuario.
- Se deben identificar los activos de información, valorarlos según su criticidad, identificar la información sensible y su almacenamiento, retención y recuperación para cada proyecto.
- Es responsabilidad del líder del proyecto y líder técnico garantizar el cumplimiento de los lineamientos generales.

1.2 Criptografía y comunicaciones – (Certificados y Firmas Digitales)

- Los sistemas de información expuestos en internet o alojados en la nube deben contar con certificados digitales (https), con claves públicas como mínimo RSA 2048 Bits; para garantizar la identificación de XM en internet, protección de usuario y contraseña en redes públicas y cifrado de comunicaciones. Es responsabilidad de cada proyecto el contemplar los costos de adquisición de los certificados.
- Se deben utilizar firma digital en los proyectos donde se necesite garantizar el emisor de las comunicaciones entrantes y salientes. Las firmas digitales deben seguir el estándar X.509. Es responsabilidad de cada proyecto el costo y la adquisición de estos.
- Se deben contar con canales de comunicación seguros para el intercambio de información con los proveedores. (https, ftps, sftp.)
- Los sistemas de información o servicios que intercambien información con sitios, direcciones públicas o privadas por medio de internet o conexiones dedicadas deben contar con protecciones tipo proxy, firewall o vpn.

1.3 Desarrollo

- Se deben realizar casos de prueba para la identificación de riesgos en los mecanismos de entrada de información que permitan la detección de vulnerabilidades del tipo SQL injection, Cross Site Scripting XSS, buffer overflows.
- Se debe analizar y validar el nivel de vulnerabilidad de los complementos o servicios desarrollados por terceros y que son reutilizados.
- Se debe realizar pruebas de análisis de código estático para validar el Top ten OWASP.

1.4 Ambientes de pruebas y calidad

- Los equipos (Servidores, estaciones de trabajo, equipos de infraestructura) que están en los ambientes de pruebas y calidad deben contar con protecciones de seguridad similares al ambiente de producción.
- Se deben definir modelos de autenticación y autorización de usuarios que utilicen grupos del directorio activo diferentes a los que se utilizan en el ambiente de producción.
- Los equipos de terceros, servidores o estaciones de trabajo, que se ingresen a los ambientes de pruebas o calidad deben cumplir los requisitos contemplados para equipos de terceros.
- Los equipos de terceros tipo appliance (combinación de hardware y software para realizar una tarea específica) deben contar con la aprobación del responsable de seguridad tecnológica en el equipo de operación.

2 Seguridad en Infraestructura

- Toda la infraestructura tecnológica que ingrese a XM en los distintos ambientes (pruebas, calidad o producción) debe ser provista con las líneas base de seguridad tecnológicas.
- Se debe tener implementado control de código malicioso (antivirus, antimalware, antispam) en todos los equipos de usuario final.
- Se debe definir la ubicación física y lógica (DMZ, red interna y segregación de funciones) de los servidores con el fin de no exponerlos.
- Se debe definir el esquema de monitoreo de equipos o servicios críticos.
- Se debe definir el esquema de continuidad de todos los equipos críticos que ingresen nuevos.
- Se debe realizar análisis de vulnerabilidades de los nuevos componentes de la plataforma tecnológica antes de ingresar a producción.
- Las aplicaciones deben asegurar el envió de correo electrónico únicamente por medio de los servidores SMTP autorizados por XM.

3 Auditorias

La auditoría dentro de las aplicaciones se desarrollara según lo indicado en el documento de requisitos para el proyecto.

- XM tiene disponible las siguientes tecnologías de log:
    - Logs nativos de servidores.
    - Logs nativos de equipos de comunicaciones.
    - Auditorias nativas dentro de SQLServer.
    - Auditorias de base de datos Oracle.

    Nota: El tiempo de almacenamiento de estos log esta definidos con el proveedor de infraestructura en disco y en cinta.
- Se debe identificar por parte de los proyectos los logs críticos asociados aplicación, infraestructura y base de datos.
- Todo proyecto debe definir el tiempo de almacenamiento y retención de los log de auditoria y logs de excepciones técnicos y de negocio propios de la aplicación(es) desarrolladas, en caso

de ser diferentes a los tiempos pactos con el almacenamiento y retención en con el área de infraestructura.

4 Entrega de datos

- Se validará la clasificación de información del negocio antes de ser entregada a terceras partes, con el fin de identificar controles para su protección y mitigación de riesgos.
- Cuando se trate de información sensible o confidencial es indispensable que previamente se haya firmado un acuerdo de confidencialidad entre las partes y se cuente con la autorización formal del directivo correspondiente.
- No se entregaran datos con una vigencia inferior a 1 mes en el caso que se tenga información clasificada como confidencial con el fin de cumplir con la regulación. En caso de necesitarlo se debe excluir la información confidencial de éstos.
- Bases de datos ORACLE
  - Se entregara copia de las estructuras y datos que se requieran para el proyecto, previa autorización del Directivo del proceso en el que se desarrolla el proyecto.
- Base de datos SQLserver
  - Se entregara copia de las estructuras y datos que se requieran para el proyecto, previa autorización del Directivo del proceso en el que se desarrolla el proyecto.
- Migración de datos al ambiente de pruebas.
  - ORACLE: Se realiza la actualización de las estructuras y los datos según solicitud del proyecto en desarrollo. Para la parte operativa se seguirá el procedimiento descrito en los procedimientos de mantenimiento y soporte de infraestructura. Este procedimiento se le explicará al proveedor que este participando en el proyecto.
  - SQLServer: Se realizara la actualización de los datos a petición del proyecto en desarrollo. Para la parte operativo el proyecto deberá entregar los scripts que correspondan para la migración de los datos necesarios para el proyecto.
  - Para ORACLE y SQLServer es necesario asignar los permisos correspondientes según el procedimiento del proveedor de mantenimiento y soporte de infraestructura.

NOTA: En caso de requerirlo se deben definir controles de seguridad adicionales según la complejidad del proyecto a desarrollar.

Referencias

- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013
- OWASP Testing Guide v4
- NIST Special Publication 800-53 Revision 4
- Official (ISC)²® Guide to the CISSP® CBK®, Fourth Edition