	POLÍTICA CORPORATIVA DE ASEGURAMIENTO DE LOS SISTEMAS DE INFORMACION	Código COR.S5.4.3.PO.003	
		Página 1 de 6	Versión: 2.0
Proceso: Seguridad de Información		Sub-proceso: Controles de seguridad IT	

Elaborado por: Martin Valdivia Director Asociado IT de Seguridad	Revisado por: Carmen Soto Director Corp. de Soporte e Implementación de Soluciones Carlos Osorio Director de Sistemas Daniel Alvan Gerente Corp. IT Negocios Industriales. Edwin Hidalgo Líder Integración IT Francisco Frez Director Corporativo de Infraestructura, Soporte y Seguridad Giulianna Carranza Director Asociado de Inteligencia de Negocios Jorge Pueyo Director Corporativo IT Negocios Comerciales Luis Kitayama Director Corp. Centro Integración y Desarrollo Luis Watanabe Director A. Corp. IT Nueva Tecnología y Arquitectura	Aprobado por: Arturo Sessarego Gerente Corporativo Senior de Tecnología de Información	Fecha de Emisión: 29.08.14
---	--	---	-------------------------------

1. PROPÓSITO


Definir los requisitos mínimos de seguridad que todo Sistema de Información usado en YANBAL INTERNATIONAL debe cumplir para minimizar los riesgos de la seguridad de la información.

2. ALCANCE

La presente política es de cumplimiento obligatorio para todo sistema de información que sea usado en YANBAL INTERNATIONAL, independientemente si es desarrollado de manera interna o externa, si es adquirido a un tercero o si es alojado de manera interna o externa en redes, incluidos los servicios de hosting o en la nube.

3. DEFINICIONES

- 3.1 **Autenticación:** Proceso utilizado para verificar la identidad de un usuario. Normalmente la autenticación se da con contraseñas.
- 3.2 **Autenticación de Doble Factor:** Requerimiento del ingreso de 2 evidencias para verificar la identidad del usuario. Típicamente requiere el ingreso de una contraseña y de un passcode generado por un token.
- 3.3 **Código Captcha:** Se trata de una prueba desafío-respuesta en la que un usuario introduce correctamente un conjunto de caracteres que se muestran en una imagen distorsionada que aparece en pantalla.
- 3.4 **Cuenta de usuario:** Se refiere a la identificación del usuario ante un Sistema de Información.
- 3.5 **Datos Críticos:** Datos clasificados como secretos o confidenciales según lo definido en la Política Corporativa de Clasificación de Información así como los datos personales y/o sensibles tal como están definidos en la Ley 29733 de Protección de Datos Personales.


	POLÍTICA CORPORATIVA DE ASEGURAMIENTO DE LOS SISTEMAS DE INFORMACION	Código COR.S5.4.3.PO.003	
		Página 2 de 6	Versión: 2.0
Proceso: Seguridad de Información		Sub-proceso: Controles de seguridad IT	

- 3.6 **Hardcode:** Referencia a una mala práctica en el desarrollo de software que consiste en incrustar datos directamente en el código fuente del programa, en lugar de obtener esos datos de una fuente externa como un archivo de configuración o tablas del Sistema de Información.
- 3.7 **OWASP:** Acrónimo de Open Web Application Security Project. Es un proyecto de la Fundación OWASP dedicada a determinar y combatir las causas que hacen que el software sea inseguro.
- 3.8 **SaaS:** Acrónimo de Software as a Service. Software como Servicio. Se refiere al modelo de distribución de software donde el software y los datos se manejan desde los servidores de una compañía especializada de tecnologías de información y comunicación (TIC), a los que se accede con un navegador web desde un cliente, a través de Internet.
- 3.9 **Segregación de funciones:** Es una práctica en la que ningún colaborador o área debe manejar todos los aspectos o fases de una misma transacción, desde el comienzo hasta el final, con la finalidad de poder detectar los errores involuntarios, y para que ninguna persona se halle en posición de poder cometer un acto ilegal y ocultar su acción, sin confabularse con otros miembros de la Corporación.
- 3.10 **Usuario:** Colaborador o tercero que usa un recurso de información en el desempeño de sus funciones y para el logro de los objetivos de negocio.

4. POLÍTICA

Sobre la Seguridad del Sistema de Información.

- 4.1 Todo Sistema de Información contará con un modulo de seguridad que permita definir los accesos de los usuarios.
- 4.2 El Sistema de Información permitirá que el acceso a los subsistemas, módulos, sub módulos, transacciones, menús, opciones, y cualquier otro componente del mismo, esté basado en un modelo de control de acceso basado en roles (RBAC) que permita la adecuada segregación de funciones.
- 4.3 El módulo de seguridad del Sistema de Información permitirá el acceso solamente al personal asignado como Administrador del Sistema.
- 4.4 El Sistema de Información permitirá definir usuarios y contraseñas en forma individual para todo usuario a quien se le requiera otorgar acceso.
- 4.5 El Sistema de Información denegará el acceso simultáneo de un mismo usuario desde dos o más estaciones de trabajo.
- 4.6 El Sistema de Información contará con un mecanismo de bloqueo de sesión por inactividad de los usuarios que se activará de acuerdo a un tiempo de inactividad configurable. Una vez activado, el sistema de información solicitará al usuario que provea su contraseña nuevamente para desbloquear la sesión.
- 4.7 El Sistema de Información contará con un mecanismo de cierre de sesión por inactividad prolongada de los usuarios que se activará de acuerdo a un tiempo de inactividad prolongada configurable. El Sistema de Información al cerrar la sesión liberará todos los recursos que estuviese utilizando.
- 4.8 El Sistema de información no debe contener *hardcodes* de cuentas de usuario ni contraseñas, ni debe usar palabras reservadas dentro del código fuente.

	POLÍTICA CORPORATIVA DE ASEGURAMIENTO DE LOS SISTEMAS DE INFORMACION	Código COR.S5.4.3.PO.003	
		Página 3 de 6	Versión: 2.0
Proceso: Seguridad de Información		Sub-proceso: Controles de seguridad IT	


- 4.9 El Sistema de información evitará grabar archivos de configuración con parámetros generales del Sistema de Información a utilizar por el sistema, en los equipos locales de los usuarios. Por ejemplo archivos *host.ini*.
- 4.10 Los archivos de configuración del Sistema de Información deben estar aislados para garantizar la confidencialidad e integridad de los parámetros almacenados.
- 4.11 El Sistema de información no permitirá ejecutar transacciones directamente a la Base de Datos desde mecanismos provistos por el sistema tales como línea de comandos.
- 4.12 El Sistema de información deberá permitir revisar los privilegios de acceso de los usuarios.

Sobre las contraseñas de usuarios.

- 4.13 La autenticación de contraseñas de usuarios de *Staff* deberá integrarse al *Directorio Activo* Corporativo.
- 4.14 En caso de que no sea posible la integración con el *Directorio Activo*, las contraseñas deben estar sujetas a los mismos controles que las contraseñas de *Directorio Activo* y deberá exigir que el usuario cambie la contraseña inicial asignada.
- 4.15 La autenticación con contraseñas para las consultoras independientes y/o directoras independientes deberá contar con características mínimas de seguridad.
- 4.16 El Sistema de Información permitirá que el usuario cambie la contraseña asignada en cualquier momento.
- 4.17 El Sistema de Información no permitirá el almacenamiento de contraseñas de los usuarios de manera local.
- 4.18 El Sistema de Información bloqueará por 5 minutos a los usuarios que no puedan ingresar correctamente su contraseña después de 5 intentos de autenticación fallidos.
- 4.19 Las contraseñas deberán almacenarse de manera encriptada.

Sobre los controles de protección de datos del sistema.

- 4.20 El Sistema de Información deberá contar con validaciones de entrada de datos en los formularios de ingreso para asegurar la integridad de los datos ingresados.
- 4.21 El Sistema de Información deberá contar con controles de procesamiento para asegurar la integridad de los datos procesados.
- 4.22 El Sistema de Información deberá ser capaz de gestionar la encriptación y desencriptación de datos críticos que son gestionados por el Sistema.
- 4.23 El Sistema de Información deberá permitir que la definición de llaves criptográficas manejadas por el Sistema sean gestionadas de manera segura.
- 4.24 La exportación de datos del Sistema de Información a archivos con otros formatos que contengan datos críticos requerirán de un control de protección de la confidencialidad de dichos datos y de mecanismos de verificación de la integridad del archivo generado.

	POLÍTICA CORPORATIVA DE ASEGURAMIENTO DE LOS SISTEMAS DE INFORMACION	Código COR.S5.4.3.PO.003	
		Página 4 de 6	Versión: 2.0
Proceso: Seguridad de Información		Sub-proceso: Controles de seguridad IT	

Sobre los controles de protección en Internet.


- 4.25 Todo Sistema de Información Web en Internet deberá contar con un certificado digital y conexión segura.
- 4.26 Todo Sistema de Información Web en Internet debe contar con controles contra las amenazas definidas por la Open Web Application Security Project (OWASP) y debe cumplir las practicas recomendadas vigentes del estándar OWASP Software Assurance Maturity Model y en la guía OWASP Secure Coding Practices Quick Reference Guide.
- 4.27 Todo Sistema de Información Web en Internet deberá permitir trabajar con un mecanismo de protección tal como un proxy reverso.
- 4.28 Todo Sistema de Información Web en Internet deberá requerir el ingreso de un código *captcha* para el ingreso de los usuarios al sistema de información.
- 4.29 El acceso al módulo de Seguridad de un Sistema de Información Web en Internet, debe implementar un control adicional para garantizar la confidencialidad e integridad de la información del módulo. Ejemplo de ello lo constituye restricción de acceso únicamente desde direcciones IP de Yanbal o autenticación de doble factor(por ejm. con token, tarjeta de coordenadas, entre otros).
- 4.30 La información procesada por el módulo de seguridad del Sistema de Información Web en Internet deberá estar encriptada en su totalidad.
- 4.31 El Sistema de Información Web en Internet debe utilizar el puerto 443. En caso de que se requiera abrir puertos del firewall, se debe solicitar una excepción explícita por este hecho.
- 4.32 Los Sistemas de Información Web que no se publiquen en Internet deben contar con los controles definidos en el punto 4.26.

De los sistemas de información basados en SaaS

- 4.33 El Sistema de Información SaaS y la información procesada por éste, debe estar completamente aislada de la información de otros suscriptores que usan el Sistema de información SaaS.
- 4.34 Si el Sistema de Información SaaS maneja información sensible y clasificada como secreta, es preferible que dicha información sea almacenada en recursos informáticos de la Corporación.

De las aplicaciones móviles.

- 4.35 La información transmitida entre la aplicación móvil y los servidores correspondientes, será protegida de manera que se garantice la confidencialidad de la información.
- 4.36 Toda aplicación móvil que gestione información interna, deberá contar con un mecanismo de autenticación, antes de acceder a dicha información. Ejemplo de esto lo constituye la autenticación vía un servicio LDAP.
- 4.37 La aplicación móvil no deberá grabar datos críticos en el dispositivo móvil. Sin embargo, en caso de que una aplicación permita trabajar en modo off-line, se debe grabar los datos críticos de manera encriptada.

	POLÍTICA CORPORATIVA DE ASEGURAMIENTO DE LOS SISTEMAS DE INFORMACION	Código COR.S5.4.3.PO.003	
		Página 5 de 6	Versión: 2.0
Proceso: Seguridad de Información		Sub-proceso: Controles de seguridad IT	

Sobre las interfaces con otros sistemas de información

- 4.38 El intercambio de información entre Sistemas de Información deberá contar con controles criptográficos que permitan el intercambio seguro de información. Ejemplo de esto lo constituye la encriptación de los archivos transferidos y/o la protección de las carpetas contenedoras de dichos archivos.
- 4.39 El intercambio de datos del Sistema de Información con otros sistemas de información que esté basado en transferencia de archivos requerirá de la existencia de un mecanismo de control que garantice la integridad del (los) archivo(s) generado(s). Ejemplo de ello lo constituye archivos de control.

Sobre las pistas de Auditoria.


- 4.40 Todo Sistema de Información debe contar con un mecanismo de pistas de auditoría que permita asignar responsabilidad individual sobre la ejecución de las actividades realizadas en el Sistema de Información.
- 4.41 El mecanismo de pistas de auditoría como mínimo debe registrar las acciones de:
- los accesos válidos y fallidos de los usuarios y,
 - los cambios realizados a través de transacciones que contienen datos críticos.
- 4.42 El Sistema de Información debe soportar configurar la auditoria de transacciones que contienen datos críticos, los cuales serán definidos por los propietarios del proceso de negocio que es soportado por el Sistema de Información.
- 4.43 El acceso a consultar el mecanismo de pistas de auditoría debe estar separado de la funcionalidad del Sistema de Información.
- 4.44 El repositorio que almacena las pistas de auditoría debe contar con mecanismos de protección que lo protejan de accesos y cambios no autorizados. De preferencia el repositorio debe estar encriptado.
- 4.45 El periodo de tiempo de permanencia de las pistas de auditoría debe ser configurable. Como mínimo las pistas de auditoría deben permanecer 6 meses en el repositorio antes que sean eliminadas.

De la seguridad de los diversos ambientes de Operación.

- 4.46 Los ambientes en los que se cuente con datos críticos obtenidos del ambiente de Producción, deberán ser protegidos con mecanismos de protección, tales como disociación de datos.
- 4.47 Los ambientes en los que se gestione código fuente, contará con mecanismos de protección orientados a la protección del código fuente y de la propiedad intelectual de la Corporación.
- 4.48 En caso que la conformación de grupos de usuarios este integrada al Directorio Activo, se debe configurar grupos para cada uno de los diversos ambientes, de tal manera que no se comprometa la seguridad de la información de los demás ambientes.

Sobre el respaldo de la información relacionada al Sistema de Información.

- 4.49 El Sistema de Información deberá contar con un mecanismo de respaldo de la configuración del sistema.

	POLÍTICA CORPORATIVA DE ASEGURAMIENTO DE LOS SISTEMAS DE INFORMACION	Código COR.S5.4.3.PO.003	
		Página 6 de 6	Versión: 2.0
Proceso: Seguridad de Información		Sub-proceso: Controles de seguridad IT	

- 4.50 En caso de que el Sistema de Información incluya los programas fuente, se deberá contar con un mecanismo de respaldo de dichos programas.

De las excepciones

- 4.51 Toda excepción a la presente política necesariamente requerirá de la autorización del área de Seguridad IT Corporativa.

Sanciones aplicables

- 4.52 El incumplimiento de la presente política determinará la aplicación de una sanción de acuerdo a lo establecido en la política de sanciones relacionada a Seguridad de la Información.