Guía de Blindaje General de Seguridad

Versión	Descripción del cambio	Fecha
1.0	Documento original	15/09/2015
2.0	Actualización documento – uso público	29/03/2018
3.0	Actualización documento – uso público	13/12/2021
4.0	Actualización documento – uso público	18/04/2024

En fiel cumplimiento de controles de adheridos a la ***Normativa Corporativa de Seguridad de información***, a continuación, se presentan las medidas/consideraciones/bastionado de seguridad que deben cumplir toda plataforma tecnológica, sistema de información y desarrollos a ser implementados en Telefónica Ecuador.

PROTOCOLO / TECNOLOGÍA	MEDIDA	Ámbito de aplicación
Antivirus	➢ Los sistemas deben tener instalado software antivirus perteneciente a un fabricante reconocido tecnológicamente.	A TODO ACTIVO (Sistema Operativo; elemento de Red)
Parches de Seguridad	➢ Los sistemas deben ser implementados con todos los parches de seguridad estables a la fecha de implementación ➢ No se permite el uso de componentes con vulnerabilidades conocidas (obsoletas) o sin soporte de fabricante	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
Gestión de Usuarios	➢ Mínimo dos perfiles con diferentes privilegios. ➢ No utilizar usuarios por defecto. ➢ Deshabilitar sesiones nulas. ➢ Determinar un tiempo para el logout automático de conexiones/sesiones. ➢ No permitir conexiones multisesión. (conexión de un mismo usuario desde varias PCs) ➢ Viablidad para integrarse a un IdP corporativo mediante protocolos de autenticación seguros (OpenID, Oauth 2.0, Saml 2.0)	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
Gestión de Contraseñas	➢ Parametrización de contraseñas que cumplan la política interna de Telefónica (mínimo 12 caracteres, mayúsculas, minúsculas, números y caracteres especiales). ➢ Caducidad de las contraseñas. ➢ No asociar la contraseña a la institución o plataforma (No predecibles o triviales, no contraseñas por defecto) ➢ Bloqueo por intentos fallidos. ➢ Se recomienda utilizar un factor alterno de autenticación. En el caso de OTP (One Time Password) deben ser generados aleatoriamente, tener mínimo 6 caracteres, caducar y configurarse un número de intentos fallidos.	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
Telnet	➢ Deshabilitar telnet. Para administración remota utilizar SSHv2	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
SSHv2	➢ Deshabilitar SSH v1 ➢ Parametrización Segura de SSH ➢ Deshabilitar el acceso a usuarios sin contraseña ➢ Eliminar el soporte a algoritmos de cifrados basados en RC4, AES-128.	A TODO ACTIVO (S.O.; Software; elemento de Red;)
SNMP	➢ Cambiar el nombre de las comunidades “Public” y “Private” por nombres que sean difícil de averiguar. ➢ Se debe utilizar snmp v3 únicamente. ➢ Si no soporta snmp v3 (justificar), utilizar snmp_v2c cumpliendo el punto gestión de contraseñas para las comunidades ➢ Utilizar permisos solo de lectura, no se permite de escritura ➢ Controlar mediante ACLs las IPs que pueden consultar por snmp. (Filtrado de Red).	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
NTP	➢ Debe estar habilitado ntp y controlado el acceso solo al servidor configurado.	A TODO ACTIVO

	➢ La configuración de NTP debe de utilizar como servidores los propios de Telefónica. ➢ Deshabilitar el comando monlist en caso de que venga habilitado por defecto	(S.O.; Software; elemento de Red; Aplicativo)
FTP	➢ En caso de que no provea cifrado por SSL (FTPs), sustituirlo por SFTP ➢ Para transferencias de archivos utilizar SFTP o SCP ➢ Deshabilitar el servicio de FTP por defecto.	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo
mDNS	➢ Si no se está utilizando, deshabilitar este servicio	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
SMB / SAMBA	➢ Habilitar la firma de paquetes (“SMB MESSAGE SIGNING”) ➢ Deshabilitar el acceso con sesiones nulas o de invitado	SMB a Windows Servers SAMBA en Linux Servers
RDP	➢ Configurar para que se utilicen métodos de cifrado fuertes en Remote Desktop ➢ Configurar para que el uso de NLA o SSL sea obligatorio	Windows Servers
HTTPS	➢ Eliminar los soportes a SSLv2 y SSLv3, mantener TLS1.2 o TLS1.3. ➢ Eliminar el soporte a algoritmos de cifrados débiles RC4, ARC, y el cifrado por bloques EBC, CBC. ➢ Eliminar las suites de cifrados con algoritmos síncronos cuyas claves sean menores a 256 bits. ➢ Eliminar las suites de cifrados con algoritmos de HASH los cuales sean MD4, MD5, SHA1. ➢ En las aplicaciones web deben instalarse certificados digitales emitidos por una entidad certificadora CAs reconocidas con firmas SHA2RSA o superiores. No deben estar caducados.	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
Puertos sin uso	➢ Toda interfaz o puerto (físico / TCP / UDP) que no se utilice deberá estar cerrado o desactivado.	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
Trazabilidad y Auditoria	➢ Debe estar habilitado logs de auditoría y seguridad a un nivel que permita tener trazabilidad de origen (IP/Usuario), acciones realizadas, fecha y hora (timestamp).	A TODO ACTIVO (S.O.; Software; elemento de Red; Aplicativo)
Integración a SIEM	➢ Habilitar el envío de logs a servidor de gestor de eventos (SIEM)	Aplicaciones por determinar (S.O.; Software; elemento de Red)
Aplicación Web	➢ Limitar el tamaño de entrada y tipos de datos (Inyección de código malicioso) mediante listas blancas. ➢ Habilitar el control de autenticación y gestión de sesiones de usuarios. Deben tener un nivel de autenticación y autorización. ➢ Evitar exponer datos sensibles/confidenciales en el portal web. ➢ Deshabilitar configuraciones por defecto, paginas de ejemplo, de pruebas, de respaldos, de administración o acceso a directorios. ➢ Todo parámetro relacionado a información sensible como claves no debe ser configurado en hard-code. Esta tipo de información debe ser obtenida desde backend. ➢ Solo debe publicarse el código en modo "release". Los componentes compilados en modo “debug”, como los *.pdb no deben existir en entornos productivos. ➢ Revisar el tipo, tamaño y extensión de todo fichero que requiera ser cargado (upload) al servidor de aplicación. No se debe permitir la carga de archivos ejecutables.	A desarrollos de aplicaciones Web

	➢ Los mensajes de aviso o error que presente una aplicación no deben contener ningún detalle técnico. ➢ Incluir cabeceras de seguridad HTTP la cuales previenen de fugas de información y ciertos tipos de ataques informáticos.	
Aplicación Móvil APPs	➢ Implementar mecanismos de identificación y autenticación de los usuarios. ➢ Caducar la sesión de los usuarios después de un tiempo determinado. ➢ Las aplicaciones deben instalarse y ejecutarse en dispositivos móviles con sistemas operativos actualizados. ➢ Implementar controles de seguridad para evitar la depuración, ejecución de ingeniería inversa, manipulación de ficheros de configuración. ➢ Debe estar firmada y provisionada con un certificado digital válido. No habilitar el esquema de firmas v1. ➢ No almacenar información confidencial o sensible de la aplicación en el dispositivo móvil ni tampoco en el código fuente. ➢ Solamente ejecutar los permisos mínimos requeridos en el dispositivo móvil. (Por ejemplo evitar la ejecución del permiso "Write External Storage") ➢ No utilizar notificaciones del tipo SMS, MMS o similares para enviar datos sensibles desde/hacia los dispositivos móviles. ➢ La comunicación desde la app a servicios de terceros como APIs se debe realizar de manera cifrada como el protocolo HTTPS. ➢ Debe utilizarse un esquema de ofuscación apropiado y robusto contra tácticas de desofuscación manual y automatizada	A desarrollos de aplicaciones móbiles
Webservices y APIs	➢ Los endpoints deben ser expuestos exclusivamente mediante HTTPS. ➢ Implementar mecanismos de autenticación y autorización para consumir los webservices. Renovar claves y tokens de acceso periódicamente. ➢ Configurar protocolo de comunicación segura HTTPS v1.2 o superiores. ➢ Permitir el uso de los métodos HTTP necesarios en cada endpoint. y restringir al resto de métodos. ➢ Realizar la validación de datos de entrada analizando tamaño, rango, formato y tipo. ➢ Controlar la información confidencial enviada en los requests y responses HTTP como contraseñas, tokens, API keys, entre otros no deben aparecer en la URL. Utilizar mecanismos de cifrado para proteger la información confidencial.	A desarrollos de APIs
NFS	➢ No compartir archivos o file systems en servidores ➢ Los archivos que sea obligatorio su compartición deben tener restricción de accesos y tener una justificación técnica. ➢ Evitar compartir con permisos de Escritura. ➢ Habilitar mecanismo seguro de transferencia de archivos (sFTP o SCP)	Aplicaciones por determinar (S.O.; Software; elemento de Red)
Entornos de Cloud	➢ Toda plataforma o servicio web en Cloud deberá cumplir con Estándares de Seguridad reconocidos como la ISO27017/27018/ ISO27701. ➢ Deberá contar con reportes de seguridad SOC1, SOC2. ➢ Llevar a cabo análisis de vulnerabilidades periódicos. ➢ Soportar protocolos de autenticación como (OpenID, Oauth 2.0, Saml 2.0) para integrarse al IdP.	A entornos Cloud
Datos Personales	➢ Las aplicaciones o servicios que gestionen datos personales que identifican al usuario o al cliente, deberán convenir el acuerdo DPA.	A todos los activos

	➢ Las aplicaciones deberán implementar mecanismos para proteger la confidencialidad e integridad de los datos personales.	

Estas consideraciones deberán ser ***certificadas*** por el área de Seguridad Digital en la ejecución de Proyectos para autorizar el paso a producción de los activos.