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	10/12/2021

Guía de Blindaje General de Seguridad

En fiel cumplimiento de controles 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 (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 (S.O.; Software; elemento de Red; Aplicativo)
Gestión de Usuarios	➢ Mínimo dos perfiles con diferentes privilegios. ➢ No usuarios por defecto. ➢ Listas de control de acceso o Control Plane para limitar el acceso solo a administradores. ➢ Deshabilitar sesiones nulas. ➢ Habilitar time-out de conexiones/sesiones.	A TODO (S.O.; Software; elemento de Red; Aplicativo)
Gestión de Contraseñas	➢ Parametrización de contraseñas que cumplan la política interna de Telefónica (mínimo 8 caracteres, mayúsculas, minúsculas, números y símbolos). ➢ Habilitar política de contraseñas para cumplimiento de política interna de Telefónica de manera obligatoria.	A TODO (S.O.; Software; elemento de Red; Aplicativo)

	➢ No asociar la contraseña a la institución o plataforma (No predecibles o triviales) ➢ Modificar contraseñas por defecto.	
Telnet	➢ Deshabilitar telnet. Para administración remota utilizar SSHv2	A TODO (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	A TODO (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 (S.O.; Software; elemento de Red; Aplicativo)
NTP	➢ Debe estar habilitado ntp y controlado el acceso solo al servidor configurado. ➢ 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	A TODO (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 (S.O.; Software; elemento de Red; Aplicativo
mDNS	➢ Si no se está utilizando, deshabilitar este servicio	A TODO (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 superiores. ➢ Eliminar el soporte a algoritmos de cifrados débiles como RC4, CBC, CHACHA_POLY. ➢ 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 interna o externa. Para el caso de aplicaciones expuestas en redes públicas los certificados los deben emitir entidades CAs reconocidas.	A TODO (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 (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 (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. ➢ Deshabilitar configuraciones por defecto, paginas de ejemplo, de pruebas, de respaldos, de administración o acceso a directorios.	A desarrollos de aplicaciones Web
Aplicación Móvil APPs	➢ Las aplicaciones deben instalarse y ejecutarse en dispositivos móviles con sistemas operativos actualizados. En Android deben ser versión mínima 9 o superiores. ➢ 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. ➢ Solamente ejecutar los permisos mínimos requeridos en el dispositivo móvil. (Por ejemplo evitar la ejecución del permiso “Write External Storage”)	A desarrollos de aplicaciones móbiles
Webservices y APIs	➢ 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.	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)	

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.