1 Objetivo y Alcance

Describir lo necesario para implementar la seguridad y privacidad de la información en la Universidad de Pamplona.

2 Responsable

Secretarìa General / Director CIADTI

3 Definiciones

Confidencialidad: La información debe ser clara sólo para los extremos autorizados.

Integridad: La información no debe ser alterada durante el transporte por las redes inseguras.

Continuidad: La información debe estar disponible para los usuarios auténticos.

TCP/IP: Pila de protocolos implementado por la IETF que permite la implementación de redes WAN con conmutación de paquetes por medio de direccionamiento jerárquico usando direcciones IP y que logra el transporte confiable gracias a su manejo de errores usando TCP.

RFC: Request For Comments. Documento netamente técnico emitido por la IETF que define los detalles de un protocolo involucrado en la pila de protocolos TCP/IP.

IETF: Internet Engeenering T Force. La Fuerza de Trabajo de Ingeniería de Internet

Host: Un servidor, PC, estación de trabajo o dispositivo móvil que en algún momento posee una dirección de capa de red de la pila de protocolos TCP/IP.

NAT: Network Address Translation (Traducción de Direcciones de RED). Es cuando un firewall convierte una IP de origen en una IP de destino.

IPS: Intruder Prevention System. Un sistema preventor de intrusos que permite de acuerdo a parámetros de configuración emitir alarmas y en algunos casos acciones automáticas ante ataques reconocidos.

4 INTRODUCCIÓN

Debido al gran auge en el uso de las redes para la implementación de procesos y el transporte de información, toda institución debe mantener una Política de

Seguridad de la Información que le permita afinar el esquema y lograr mejorar y tomar acciones ante hechos que de alguna forma debiliten la seguridad o amenacen alguno de elementos que caracterizan el esquema seguro.

La Universidad de Pamplona buscando implementar la ISO 27001, define esta política como parte esencial y obligatoria de esta norma y buscando cumplir con una amalgama con otros proveedores o clientes establece esta política que está enmarcada dentro de los controles recomendados por la ISO 27002. Esta política junto con el Análisis y Gestión de Riesgos a realizar en la Universidad de Pamplona harán parte junto con otros documentos recomendados en la norma y creados de forma personalizada para la Universidad e Pamplona, lograrán de forma integral la implementación de la norma ISO 27001, también teniendo en cuenta que la Universidad de Pamplona ya cuenta con la certificación en ISO 9001 y la GP 1000.

5 SERVICIOS DISTRIBUIDOS

5.1 DEFINICIONES

El término “Servicios Distribuidos” se entiende como aquellos servicios que poseen dos características: Transparencia de Ubicación y Transparencia de Acceso. Los dos van encaminados a ofrecer servicios sin que el usuario tenga necesidad de conocer detalles del sitio físico en el cuál se encuentra el servicio y a que el mismo servicio siempre se accede sobre una misma URI (Unique Resource Identifier). Los servicios que se ofrecen a través de servidores y redes de computadores en la Universidad de Pamplona cumplen estos dos parámetros por lo cual estos servicios se entenderán como servicios distribuidos.

Adicionalmente para ofrecer los servicios se han implementado desde su inicio bajo la pila de protocolos TCP/IP. Esta pila de protocolos, basada én el Modelo OSI, se ha entendido como el esquema más adecuado debido principalmente a tres factores: el acceso a la tecnología, la excelente estandarización de este esquema por parte de la IETF (La Fuerza de Trabajo de Internet) y a su sorprendente extensión a nivel mundial.

Todos los conceptos que se dan en el documento se entenderán bajo el esquema TCP/IP.

5.2 SEGURIDAD EN LOS SERVICIOS DISTRIBUIDOS

5.2.1Control de Acceso

5.2.1.1 Definición

El control de acceso hace referencia a las reglas que permiten o deniegan el acceso de una subred, un host o un grupo de hosts a un servicio o un grupo de servicios en una subred, un host o un grupo de hosts. Generalmente este elemento se implementa con la ayuda de un firewall.

Un firewall es un dispositivo hardware o hardware/software que permite implementar el elemento Control de Acceso en una red.

Los firewall tipo hardware son más especializados y por consiguiente más recomendables.

Además de las reglas de acceso ya mencionadas, un firewall permite la implementación de NATs.

Una NAT por Network Address Translation (Traducción de Direcciones de Red) permite que la dirección IP de un host sea vista como otra dirección IP por otro host. Este concepto aplica no sólo a un host, sino también a una subred o un grupo de hosts.

Existen dos tipos de NATs: estáticas y dinámicas. Una NAT estática hace que la dirección IP de un host se convierta en otra única dirección IP. Las dinámicas permiten asignar una única dirección IP a un grupo de hosts cuando se comunican con un host, una subred o un grupo de hosts determinado. Las NAT se usan con mucha frecuencia porque permiten administrar los recursos de direccionamiento IP de una red de forma centralizada y sobretodo segura. Las NAT estáticas se usan para servidores, evitando que el propio equipo tenga contacto directo con otras subredes, pero obteniendo por ejemplo una dirección válida en Internet. Las NAT dinámicas se usan generalmente cuando se hace necesario que un grupo de hosts que están en una red puedan obtener una única dirección IP ara acceder a una serie de servicios. Estos hosts no podrán ofrecer servicios como si se logra hacer con la NAT estática.

La Figura 1 y 2 presentan las NAT.

Descripción de la regla NAT	IP origen que viene en el paquete original	IP destino que viene en el paquete original	IP origen en la que se convierte	IP destino en la que se convierte
Regla para paquetes salientes enviados por el host original	192.168.0.2	*	200.21.150.3	*
Regla para paquetes entrantes enviados hacia la IP destino original	*	200.21.150.3	*	192.168.0.2

Tabla 1. Par de reglas para una NAT estática en el firewall

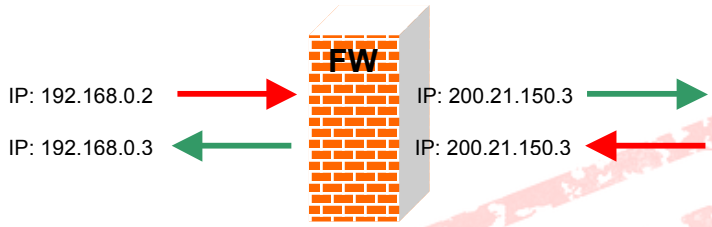

Figura 1. NAT estática

En la Figura 1 se observa como la NAT en el firewall representada en la Tabla 1 configura para que cuando el host con la IP 192.168.0.2 envíe algún paquete a cualquier destino, el valor de los campos del paquete que contengan su IP cambian su valor a la IP 200.21.150.3. Igualmente cuando desde cualquier origen se haga una petición a su IP traducida, los campos que contienen la IP de destino 200.21.150.3 cambien su valor a 192.168.0.3. Nótese que en el ejemplo el destino al cual se traduce la dirección en la primera regla de la NAT es * igual que el origen en la segunda regla de la NAT estática, lo que quiere decir que se traduce a cualquier destino o desde cualquier destino, pero en algunas ocasiones se especifican destinos más restringidos como un solo host, una subred o un grupo de hosts.

Descripción de la regla NAT	IP origen que viene en el paquete original	IP destino que viene en el paquete original	IP origen en la que se convierte	IP destino en la que se convierte
Regla para paquetes salientes enviados por el grupo de hosts original	192.168.0.2-192.168.0.7	*	200.21.150.3	*

Tabla 2. Regla para una NAT dinámica en el firewall

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

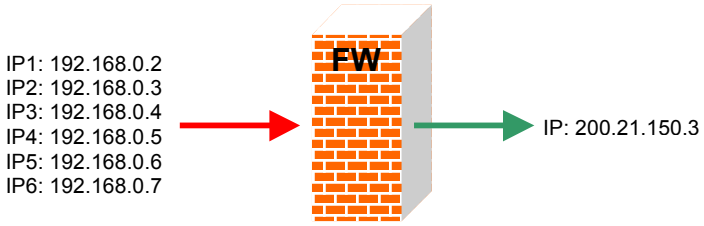

Figura 2. NAT dinámica

En este caso hay una sóla regla y es sólo para el envío de paquetes desde el grupo de hosts que pretende obtener servicios.

5.2.1.2 Política

Toda subred de la Universidad de Pamplona en donde se presten servicios debe estar protegida con un dispositivo firewall que permita implemetar el elemento Control de Acceso y debe estar configurado con las reglas y NATs pertinentes.

Los servidores deben poseer una IP interna y convertirse en IPs válidas a través de NATs.

Los accesos temporales se configurarán sólo por lapsos máximos de 24 horas.

-

5.2.1.3 Administración

Sólo los PCs de los roles Operador de Infraestructura y Coordinador de Infraestructura pueden tener acceso a administrar los firewall

Existen dos roles que pueden administrar los dispositivos para el control de acceso: Operador de Infraestructura y Coordinador de Infraestructura Tecnológica. Estos dispositivos se deben administrar desde los PCs de cada uno de los roles permitidos. Igualmente estas reglas se aplican a la administración del IDS.

5.2.2Autenticidad

5.2.2.1 Definición

La autenticación es garantizar que la información que llega a uno de los extremos de la comunicación es efectivamente de quien dice ser.

La autenticación se apoya fuertemente en el concepto de "firma digital", a su vez en el concepto de PKI y finalmente se fortalece con el concepto de certificados digitales.

PKI es la Infraestructura de Clave Pública con algoritmos asimétricos para la generación de un par de claves que se entiende como supremamente seguro al tener un componente privado y otro público.

La firma digital es aquella que se anexa a una información para garantizar que proviene del emisor correcto. Esto se logra gracias a la encripción con el componente privado de un par de claves PKI y la decripción con el componente público y finalmente a la comparación de la información desencriptada con la información íntegra enviada sin encripción.

Finalmente para fortalecer el esquema, se adquiere un certificado digital con una autoridad certificadora (verisign, certicamara, entre otras) que vincula el componente público con una información de la empresa y con este tercero denominado Autoridad Certificadora que actúa como un avalante de la veracidad de la información.

5.2.2.2 Política

En la Universidad de Pamplona los servicios que se envíen por medio seguro, es decir, usando encripción, deben presentar a su usuario un Certificado Digital que en el peor de los casos se genere en el servidor usando OpenSSL y en el mejor de los casos presente un Certificado Digital emitido por una autoridad Certificadora muy reconocida como Verisign o Certicamara.

5.2.2.3 Cumplimiento

Esta política busca cumplir con el Dominio 11. CONTROL DE ACCESO de la norma ISO 27002.

5.2.3No repudio

5.2.3.1 Definición

Se entiende como un recibido digital. Cuando se envíe una información y se haga necesario tener una verificación de ese envío, esta es la opción a usar. Va muy de la mano con la firma digital, pues el que una información se halla firmado con el componente privado de un par de claves PKI es ya garantía de que esa información fue efectivamente enviada por el emisor verdadero.

5.2.3.2 Política

En la Universidad de Pamplona cuando se reciba información importante se debe exigir su adicional firma digital y su respectivo Certificado Digital para lograr obtener una verificación del recibo de dicha información.

5.2.3.3 Cumplimiento

Esta política busca surtir el dominio 10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

5.2.4Confidencialidad

5.2.4.1 Definición

Confidencialidad es el elemento de la seguridad computacional que garantiza que sólo el receptor autorizado puede ver la información que se le envía.

Para lograr esto se usa la encriptación y una combinación de cualidades entre los algortimos simétricos y asimétricos.

Existen dos mecanismos para la encriptación, el simétrico en el que se trabaja una clave para encriptar y la misma para desencriptar y el asimétrico en el que se trabaja una clave pública para encriptar y su par privada para desencriptar. La principal ventaja de la simétrica es la velocidad de encriptación pero su gran desventaja es el riesgo al transportar la clave. La asimétrica tiene la desventaja del gran consumo de recursos al encriptar pero su mayor ventaja es que sólo el poseedor de la clave privada del par de claves es capaz de desencriptar la información que ha sido encriptada con su par pública. Por eso se usa un híbrido que combina las ventajas de las dos, encriptando las claves privadas para el transporte con la parte pública del par de claves asimétricas y luego encriptando absolutamente toda la información a transportar por medio de estas claves privadas cuyo envío ya se hizo de forma altamente segura.

5.2.4.2 Política

En la Universidad de Pamplona siempre se usará la encriptación para el transporte por las redes de información confidencial. Una de las informaciones más confidenciales es el usuario y contraseña en páginas de logueo.

5.2.4.3 Cumplimiento

Esta política cumple con el dominio 11. GESTIÓN DE COMUNICACIONES Y OPERACIONES específicamente en el objetivo 10.6.

5.2.5Integridad

5.2.5.1 Definición

Integridad de la información es lograr que los datos enviados sean recepcionados tal cual en el otro extremo.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

Para lograrlo se usan los denominados algoritmos hash como MD5 y SHA1.

5.2.5.2 Política

En todo servicio que emita la Universidad de Pamplona en cuanto a información delicada como contraseñas, notas y documentos confidenciales se debe implementar un mecanismo que use los algoritmos hash más estandarizados y modernos posibles o el mecanismo que más aplique para lograr la integridad de esta información cuando se transporta por una red.

5.2.6Firewall de Capa de aplicación

5.2.6.1 Definición

En la actualidad es necesario proteger los sistemas de información que generalmente se implementan en la web con un WAF, Firewall de Capa de Aplicación. Este dispositivo implementa OIWASP que es un proyecto adoptado y generalizado de protección de sistemas en la web.

5.2.6.2 Política

Debido a que la Universidad de Pamplona implementa sus servicios de información en la Web debe mantener un WAF de tipo appliance y con soporte.

5.2.6.3 Estado actual y configuración a seguir

La Universidad de Pamplona implementa un WAF de última tecnología con soporte.

5.2.6.4 Cumplimiento

De aplicarse la política se cumple con el dominio 10, específicamente los objetivos 10.6, 10.8 y 10.9. Permite también realizar mejores prácticas de supervisión tal como lo recomienda el objetivo 10.10 del mismo dominio.

5.2.7Disponibilidad de servicio

5.2.7.1 Definición

Este elemento se entiende como evitar que la prestación continua de un servicio en la red se vea afectada por ataques de denegación del servicio u otros ataques que eviten que un acceso normal se lleve a cabo. El mecanismo que permite lograr esto es generalmente la implementación de un IDS (Intruder Detection System).

5.2.7.2 Política

En cada subred y cuando aplique por disponibilidad de la tecnología, exigencia de los clientes o por conveniencia en la cantidad de usuarios concurrentes, debe existir un IDS que permita en el peor de los casos visualizar logs y en el mejor de los casos obtener correos electrónicos a direcciones de celular del Operador o Coordinador de Infraestructura recepcionados como mensajes de texto cuando se active una alarma.

5.2.7.3 Situación actual y configuración a seguir

La siguiente Figura nos presenta un esquema de firewalls contra subredes en la Universidad de Pamplona.

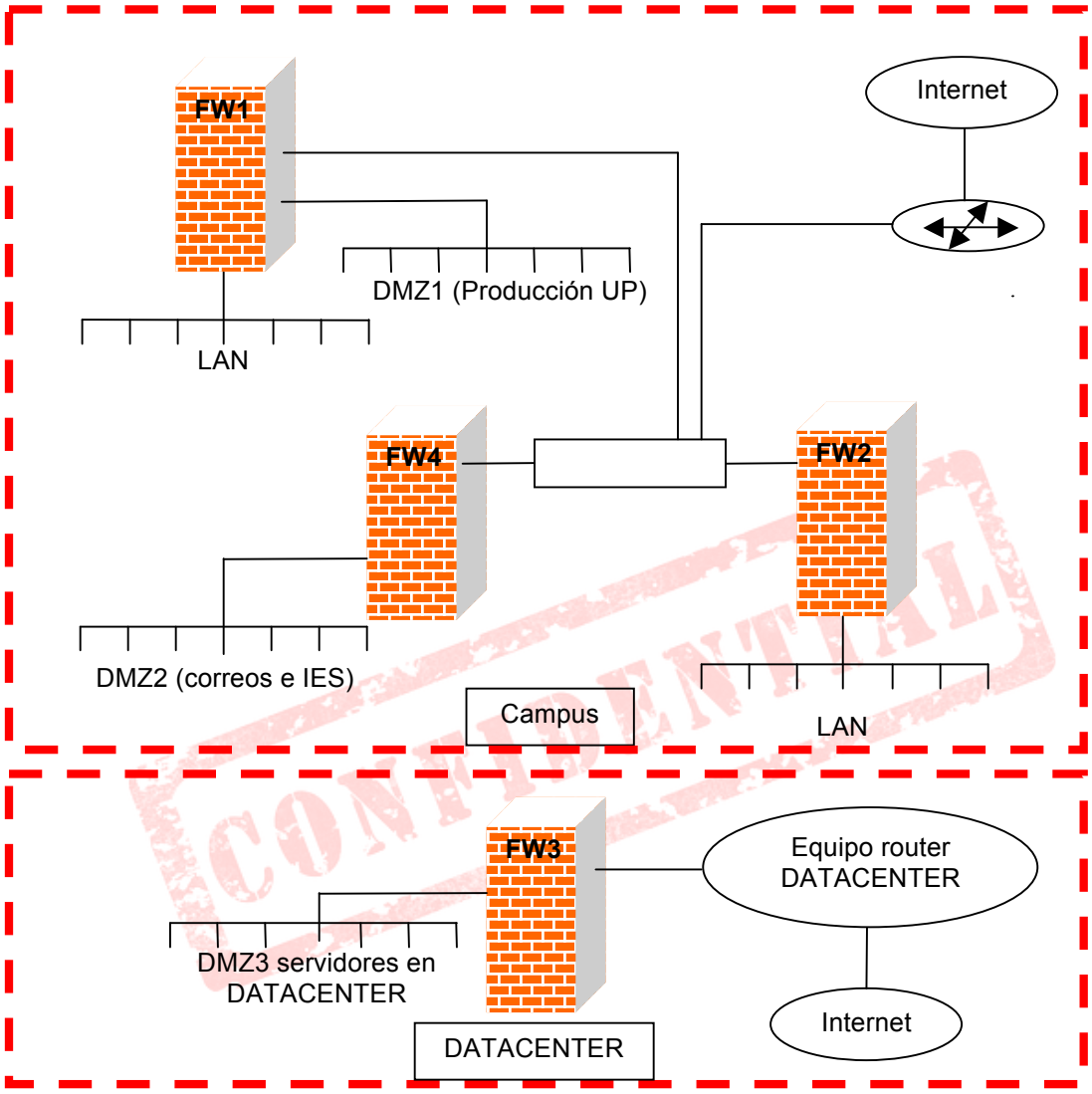

Figura 3. Firewall y subredes a nivel de firewall

Los IPS pueden ser comerciales u OpenSource. Actualmente se implementa el IPS Tipping Point y la razón de la elección es por su disponibilidad, su gran calidad y porque actualmente es el IPS más usado contando con un fuerte equipo que lo actualiza y desarrolla.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

El IPS debe estar configurado para generar logs de cada uno de los accesos que se puedan considerar riesgosos y debe generar un correo con las siguientes características:

- Dirigido a: internet@unipamplona.edu.co
- Desde: infraestructura.ids@unipamplona.edu.co
- Asunto: Alerta_de_seguridad_de_IDS_TippingPoint
- Cuerpo: El msg de la alerta (el msg es el mensage congurado para una regla de detección)

Como se observa en la Figura 3, los firewall de la institución que protegen todos aquellos ítems que podrían sufrir ataques, forman parte del esquema en el cual se tienen 4 subredes:

- DMZ1 (Servidores de producción de aplicativos)
- DMZ2 (Clúster de correo y servicios demo-beta de las IES en convenio)
- DMZ3 (Servidores de producción en DATACENTER)
- LAN (La red local en Campus)

Este esquema debe ser protegido con un IPS en cada subred.

5.2.7.4 Checklist para detección de intrusos

http://www.cert.org/tech_tips/intruder_detection_checklist.html

5.2.7.5 Cumplimiento

De aplicarse la política se cumple con el dominio 10, específicamente los objetivos 10.4, 10.6, 10.8 y 10.10.

6 ADMINISTRACIÓN DE CONTRASEÑAS

6.1 CARACTERÍSTICAS DE LAS CONTRASEÑAS

6.1.1 Política

Las contraseñas para logueos a servicios deben: no ser débiles, no ser las contraseñas por defecto, no ser la misma para varios sistemas y no reusarse a lo largo del tiempo.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

Debido a los mecanismos que el atacante puede usar para escanear accesos en la red, siempre se usarán métodos de encriptación para hacer logueos de administración usando software estándar, probado y extendido. Un buen ejemplo es OpenSSH.

6.1.2Definiciones

6.1.2.1 Contraseñas débiles

6.1.2.1.1 Características

- Están en un diccionario de datos. Ejemplos: luna, tierra, mesa, etc
- Nombres propios: carlos, Carlos, CARLOS, Martha, etc
- Nombres famosos reales o imaginarios: NASA, Coca-Cola
- Acrónimos del ámbito informático: IDF, TCP, IAPP, etc
- Variaciones o combinaciones simples de los nombres: acorrea, abcarrascal, etc
- Tienes menos de 6 caracteres de longitud

6.1.2.1.2 Recomendaciones

- No mantener las contraseñas en archivos sin encriptación
- Una buena heurística para escoger un password es seleccionar una frase fácil de recordar, como “Arbol Que Nace Torcido Jamás Su Tronco Enderezará”´, y usar las primeras letras para formar el password, usando algunos caracteres especiales y mezclas de mayúsculas y minúsculas. Para el ejemplo de la frase de arriba, una contraseña podría ser: aQn{tjs*te. Por ningún motivo use esta contraseña de ejemplo como una contraseña en el sistema.
- Crear contraseñas de 6 caracteres o más en todos los niveles de acceso.

6.1.2.2 Contraseñas por defecto

Los intrusos explotan la vulnerabilidad de los sistemas que se han instalado con contraseñas por defecto y que no han sido cambiados, incluyendo aquellos que se instalan con contraseñas por defecto de un fabricante y en ocasiones no tienen contraseña asignada por defecto. El siguiente incidente reportado por la organización CERT muestra un ataque usando esta vulnerabilidad: http://www.cert.org/incident_notes/IN-98.01.irix.html. Este concepto aplica

igualmente a los equipos de red o comunicaciones, en general, a todos los equipos que se puedan administrar usando la combinación usuario y contraseña.

6.1.2.2.1 Recomendaciones

- Cambiar todas las contraseñas por defecto de los sistemas, no usando "contraseñas débiles". Esta recomenda
- Siempre que se realicen actualizaciones en un sistema se debe verificar que no se actualice a una contraseña por defecto. Si es el caso, cambiarla según las recomendaciones.
- Escanear los archivos de contraseñas para encontrar cuentas con UIDs extras con valor cero (0), cuentas sin password o nuevas entradas en el archivo de contraseñas. No se deben permitir cuentas sin contraseña. Remuévanse las cuentas que no se usen. Para deshabilitar una contraseña en UNIX se da un valor de * a la contraseña en el archivo /etc/passwd y el shel se configura a /bin/false, eso evita que un intruso pueda acceder desde un sistema remoto a través de la red.

6.1.2.3 Contraseñas reusables y compartidas

Ni las contraseñas excelentes son completamente seguras pues pueden ser escaneadas en la red si se van desencriptadas. Es muy común que los atacantes usen sniffers de paquetes para escanear accesos del tipo usuario y contraseña. La siguiente nota de incidente de la organización CERT detalla un ataque de este tipo: http://www.cert.org/incident_notes/IN-99-06.html.

6.1.2.3.1 Recomendaciones

- No se debe usar la misma contraseña para varios sistemas pues al lograr comprometer un sistema el atacante tendrá acceso a todos los demás que posean la misma contraseña.
- No se deben reusar contraseñas a lo largo del tiempo para evitar que una contraseña anterior que esté comprometida pueda permitir un acceso.
- Es obligatorio usar mecanismos de encriptación implementados mediante software estándar y probado, de los cuales uno muy representativo es el openssh: http://www.ssh.con/index.html, http://www.openssh.com/.

6.2 ADMINISTRACIÓN DE CONTRASEÑAS DE ADMINISTRADORES EN SERVIDORES Y APLICATIVOS

6.2.1Política

Sólo los roles Operador de Infraestructura y Coordinador Técnico de Infraestructura pueden administrar las contraseñas en servidores y equipos de comunicación, siguiendo las recomendaciones acerca de contraseñas seguras.

Sólo los roles designados en los manuales de sistema de los aplicativos pueden configurar las contraseñas de administración en los aplicativos.

En la instalación, actualización, diseño e implementación de los sistemas se debe configurar la "obligatoriedad" para que no se puedan ingresar contraseñas débiles.

Esta obligatoriedad se debe extender al cambio periódico de contraseñas, en lapsos de máximo tres meses.

6.3 ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIOS FINALES

6.3.1Política

El usuario final podrá cambiar su contraseña a través del servicio que se le preste.

El sistema debe estar diseñado para no permitir contraseñas débiles cuando el usuario cambie su contraseña.

6.4 Cumplimiento

Esta política permite acompasarse con la norma ISO27002 en las recomendaciones dentro del dominio 11. CONTROL DE ACCESO, específicamente en los objetivos de control 11.2, 11.3, 11.5.

7 LOGS

7.1 DEFINICIÓN

Un log (o bitácora) permite que se haga seguimiento a las actividades realizadas sobre un servicio en un rango de fechas y horas.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

7.2 POLÍTICA

Todo sistema que se implemente debe mantener un log liviano en texto puro y se deben establecer los mecanismos de periocidad, detalle y respaldo de dichos logs con un mínimo de 12 meses.

Estos logs deben guardar el usuario, la fechahora, la IP de origen de la acción y el máximo detalle de la acción.

Los sistemas para los cuales se deben mantener logs son: 1. Administración de servidores por ssh, webmin y sftp, 2. Aplicativos, 3. Bases de datos.

7.3 Cumplimiento

Esta política permite cumplir con el dominio 10, y específicamente el objetivo de control 10.10.

8 ENLACE CON OTROS PROVEEDORES

8.1 DEFINICIÓN

La Universidad de Pamplona cuya misión es la educación, se sirve de proveedores especializados por ejemplo para la provisión de Internet, Data Center o Computación en la Nube. En ese orden de ideas este apartado define la política a tener en cuenta para garantizar que la comunicación y las interfaces entre el proveedor y el cliente sigan permitiendo que se cumplan las condiciones para la seguridad de la información.

8.2 POLÍTICA

Todos los servicios y elementos instalados en Data Centers externos deberán seguir todas las políticas recomendadas en este documento.

Para el acceso físico a las instalaciones del Data Center externo se deben seguir las políticas diseñadas por el proveedor cumpliendo a cabalidad con los formatos y recomendaciones de este proveedor. Los formatos a saber deben contener información precisa de las personas a ingresar y su vinculación con la Universidad de Pamplona. Deben ser autorizados estos ingresos por el coordinador del área en la Universidad de Pamplona que haya sido reportado al proveedor como responsable. Los permisos

serán solicitados solo desde el correo del área informado al proveedor. Se debe también informar en detalle las actividades a realizar, las fechas y horas de trabajo. Los permisos no deben hacerse para lapsos mayores a quince días o en un lapso menor si así lo establece el proveedor.

Para administrar los servidores instalados en Data Center externos, se hará con contraseñas seguras según la recomendación en este documento.

Los servicios de administración deben ser accedidos sólo desde computadores aprobados por el coordinador del área hacia las personas encargadas de administrar los firewall y siguiendo las recomendaciones de control de acceso en este documento.

Para subir información a los servidores con el fin de agilizar instalaciones o colocar información relevante en los servidores como archivos que hayan subido usuarios finales, se podrán activar servicios FTP o SSH siguiendo las recomendaciones de control de acceso y contraseñas seguras en este documento. Estos accesos deben ser controlados e informados por el coordinador del área en la Universidad de Pamplona. Se debe crear un usuario para cada cliente y para cada proceso para evitar pérdida de confidencialidad o destrucción intencional y no intencional.

Los servidores deben mantener configurado la solicitud de logueo una vez han pasado 5 o más minutos de inactividad atendiendo a recomendaciones de estándares de la seguridad de la información en cuanto a equipos desatendidos.

La Universidad de Pamplona cumplirá a cabalidad con todas las políticas emitidas y exigidas por os proveedores de servicios de tecnología y replicará en la cadena de servicios a los clientes de la Universidad de Pamplona estas políticas.

8.3 Cumplimiento

La actual política permite cumplir con el dominio 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN, en su objetivo de control 6.2 Terceros.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

9 MANEJO DE INCIDENTES

9.1 POLÍTICA

Todo incidente de seguridad informática manifestado oficialmente debe ser tratado bajo el siguiente protocolo.

9.2 Ante evidencias en el cambio de datos en los aplicativos

9.2.1 Revisión de intrusiones

Se ejecuta el protocolo "Intruder Detection Checklist" emitido por la organización CERT en la URL: http://www.cert.org/tech_tips/intruder_detection_checklist.html. Debido a que la información en la URL se entiende siempre actualizada se hará referencia principalmente a esa dirección. Sin embargo ante problemas en conseguir esta información, se puede conseguir una copia posiblemente no actualizada en el sitio principal de infraestructura en http://infratec.unipamplona.edu.co/documentación.

Objetivo: Ver si desde IPs no permitidas se ha logrado accesar a administrar algún servidor involucrado en el proceso que presenta la anomalía. Presentar el informe de anomalías de accesos.

9.2.2 Revisión de logs de acceso en aplicativos

Aprovechando el sistema de logs implementado en cada aplicativo se hará posible la revisión de accesos delicados, muy en especial aquellos de administración.

Los logs de acceso deben poder establecer el usuario, la fechahora, y el cambio realizado. Se debe presentar el informe con las anomalías de acceso.

9.2.3 Revisión de logs de acceso en bases de datos

Las bases de datos de la Universidad de Pamplona deben permitir hacer una análisis de logs de acceso con datos como usuario de la base de datos, fechahora, acción, IP de origen de la administración.

Objetivo: Revisar si desde IPs no permitidas se ha hecho administración de las bases de datos o si existen logueos y/o acciones no permitidos en algún momento. Se debe presentar el informe con las anomalías de acceso.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

9.2.3.1 Cumplimiento

La presente política permite dar cumplimiento al dominio 13. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN.

10 MEJORAMIENTO

10.1 Política

Cada 12 meses se debe ejecutar una auditoría para evaluar el estado de la seguridad informática en la institución. Esta práctica se desarrollará siguiendo una metodología estándar actualizada. Se podría usar OCTAVE de la organización CERT (www.cert.org).

11 Documentos de Referencia

Norma ISO 27001

Norma ISO 27002

Norma ISO 27005

12 Historia de Modificaciones

Versión	Naturaleza del Cambio	Fecha de Aprobación	Fecha de Validación
0	Documento inicial	20/12/2017	20/12/2017

13 Anexo

“No aplica”.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017