LINEAMIENTOS TÉCNICOS ESTANDARES DE SEGURIDAD PARA PLATAFORMAS TECNOLÓGICAS DE LA UCSC

UNIDAD PLATAFORMAS TECNOLÓGICAS - DIRECCIÓN DE SERVICIOS INFORMÁTICOS

Revisión y Control Histórico de cambios

Fecha de Revisión	Versión	Resumen y puntos modificados	Unidad Responsable
18-01-2012	1.0	Documento inicial	Jefes Unidades DYSSA, DYSSAE y Plataformas Tecnológicas
15-04-2013	2.0	Incorporación de comentario en estándares de seguridad para aplicaciones web, de los estándares de seguridad para las aplicaciones informáticas institucionales.	Jefe Unidad DYSSAE (José Comas)
24-04-2013	2.1	Actualización del punto "2.2.4. Actualizaciones y upgrades de equipamiento", de los estándares de seguridad para la red y comunicación de datos de la UCSC.	Jefe Unidad Plataformas Tecnológicas (René Melo)
30-03-2015	3.0	Revisión y actualizaciones menores.	Jefe Unidad Plataformas Tecnológicas (René Melo)
08-09-2016	4.0	Revisión y actualizaciones menores en formato	• Jefe de Unidad PT. • Coord. Gestión de la Calidad – DSI.
26-11-2018	5.0	• Revisión del manual de lineamiento. • Actualización formato documento.	• Jefe de Unidad PT. • Coord. Gestión de la Calidad – DSI.

UNIVERSIDAD CATOLICA DE LA SANTISIMA CONCEPCION
Dirección de Servicios Informáticos

Contenido

1. Antecedentes Generales

1.1. Requisitos de la Industria

Dado que la seguridad en los sistemas de comunicación y de información se ha convertido en uno de los problemas más grandes desde la aparición, y más aún, desde la globalización de Internet, la Universidad Católica de la Santísima Concepción, por medio de la Dirección de Servicios Informáticos, ha analizado la seguridad de su plataforma tecnológica considerando los siguientes aspectos:

- Valoración de Activos a proteger de la ocurrencia de un evento que atente con su integridad
- Identificación de los riesgos que ocurra el evento.
- Estimación de la frecuencia con que ocurren los eventos.
- Cuantificar el costo de las consecuencias de la ocurrencia de un evento, el costo de corregir sus efectos, y el de prevenirla.

Como resultado del análisis, se ha generado el presente lineamiento técnico con los estándares de seguridad para las plataformas tecnológicas de la Universidad. Se estableció un conjunto de medidas, en cada una de los niveles que conforman la plataforma tecnológica institucional, con la finalidad de proteger la información institucional que está bajo la responsabilidad de la Dirección de Servicios Informáticos.

1.2. Servicios implicados

Los servicios informáticos que sustentan la plataforma tecnológica institucional y por tanto requieren formalizar los lineamientos de seguridad son:

- Diseño y mantención de redes y comunicación de datos
- Administración Servidores institucionales y plataforma tecnológica asociada
- Soporte, desarrollo y mantención de aplicaciones informáticas institucionales

2. Estándares de seguridad para la red y comunicación de datos de la UCSC

La unidad de Plataformas Tecnológicas (PT) en el área de Soporte Tecnológico, Redes y Comunicación de datos es la responsable de la seguridad de la red y comunicación de datos institucional, define las medidas para resguardar la seguridad de la plataforma informática desde la perspectiva de la comunicación de datos.

2.1. Identificación de equipamiento de redes y comunicación de datos

La unidad de PT ha identificado un conjunto de equipos a los que es necesario definir y aplicar estándares o políticas de seguridad, estos son:

- Firewall-IPS
- Wireless Controller
- Switch Core De la Red

- Switch Distribución
- Switch Acceso
- Puntos de Red y Dirección IP

2.2. Definición de estándares de seguridad para el equipamiento

La unidad de PT ha elaborado la siguiente lista de tareas aplicables para fortalecer la seguridad de los equipos de redes y comunicaciones de datos:

- Seguridad física y ambiental
- Monitoreo
- Disponibilidad de equipos
- Actualizaciones y Upgrades
- Configuración y aplicación de políticas
- Backups
- Escalamiento y consultoría a Parthner tecnológicos

2.2.1. Seguridad física y ambiental

Todos los equipos de redes y comunicación de datos que conforman la red de comunicación institucional, deben cumplir con los siguientes estándares:

- Acceso restringido y controlado.
- Mantener condiciones eléctricas idóneas de acuerdo a la norma eléctrica SECTEL
- Estar en condiciones controladas de temperatura y contaminantes que puedan comprometer su funcionamiento.
- Contar con seguridad perimetral como guardias y /o alarmas.
- Operar con claves de acceso.
- Las claves de acceso deben ser almacenadas en un archivo Excel y subidas al servidor FTP "intranet.ucsc.cl", la ubicación y permisos de acceso del archivo será permitido sólo para el Director de la DSI y Jefe de la unidad Soporte Tecnológico, redes y comunicación de datos.
- Las claves de acceso de los equipos deben ser cambiadas 1 vez al año.

2.2.2. Monitoreo

Hoy en día, las redes de datos de las organizaciones, se vuelven cada vez más complejas y heterogéneas, la exigencia de su correcta operación es cada vez más crítica para el éxito de la organización. Las redes de datos soportan muchas aplicaciones y servicios estratégicos; además, su crecimiento constante y la incorporación de nuevas tecnologías van complicando y en algunas ocasiones degradando el desempeño de la misma.

Es recomendable contar con un monitoreo y análisis de las mismas que nos asegure su correcto funcionamiento, dicha acción se ha convertido en una labor cada vez más importante y de

pro-activo. El monitoreo pro-activo permite al departamento de Redes tener un sistema que ayude a detectar problemas en la red de datos, corregirlo a tiempo y prevenir futuros inconvenientes.

Para evitar que la pérdida de servicios sea repentina, el monitoreo pro-activo se basa en la inteligencia de los equipos de red, tales como: Routers, Switches y Firewalls. Para el monitoreo de los equipos de red institucional cuentan con los siguientes software o herramientas de apoyo:

- Nagios: permite monitorear todos los swicth de la red LAN de La universidad y enlaces. (esta herramienta es administrada por la unidad de Plataformas Tecnológicas).
- ASDM: Permite monitorear los firewalls e IPS. (administrado por la unidad de Plataformas Tecnológicas y empresa NeoSecure).
- Cisco Network Assistant: permite el monitoreo y configuración de Switch, (administrado por la unidad de PT, gratuito hasta la operación de 50 equipos)
- Cisco Works: Software de Administración y monitoreo de Switch para todo el campus, (administrado por la unidad de Plataformas Tecnológicas).

2.2.3. Disponibilidad de equipos

La unidad de Plataformas Tecnológicas, como lo establece en su plan de contingencias, ha establecido la existencia de un stock mínimo de respaldo para equipos que conforman la red de datos, tales como switch y Access Point con la finalidad de que, ante la ocurrencia de alguna falla, estos equipos puedan ser reemplazados.

Detalle de equipos para contingencias:

- 1 Swicth de Distribución
- 2 Swicth de Acceso
- 2 Access Point

Alta Disponibilidad

El equipo firewall dentro de la configuración de la red institucional cumple la función de limitar los accesos desde y hacia internet, filtrando paquetes TCP/UDP, asegurando las comunicaciones de datos bajo las normas de seguridad establecidas por la Dirección de Servicios Informáticos.

La unidad de Plataformas Tecnológicas posee los equipos firewall en alta disponibilidad trabajando en modo Activo/Pasivo ante fallas, cabe mencionar que todos los equipos que están antes de los firewalls están configurados de las mismas formas (2 Reuters y 2 enlaces a Internet), es decir hay dos equipos que cumplen la misma función y en caso de falla se activa el equipo que está en pasivo.

Sin Disponibilidad Ante Contingencias

Dentro de los equipos importantes, el sistema integrado de red inalámbrica WIFI, mediante su controlador inalámbrico (Wireless Controler), no posee disponibilidad de otro equipo en estado pasivo, la unidad de Plataformas Tecnológicas deja establecido que, ante una falla de alto impacto, el proveedor tecnológico del servicio (Movistar), disponga del equipo de reemplazo necesario.

2.2.4. Actualizaciones y Upgrades de equipamiento

Para todo el equipamiento activo principalmente **swicth layer 2**[1] y **swicth layer 3**[2], la unidad de Plataformas Tecnológicas aplica los updates y upgrades según corresponda, es decir, una vez por año se revisarán las updates y upgrades en conjunto con nuestro proveedor tecnológico del servicio (Movistar), si esta revisión detecta vulnerabilidades que pongan en riesgo la seguridad de nuestra plataforma de Switch, se procederá con las actualizaciones que indique el proveedor.-

Para los equipos de mayor complejidad como lo son Firewalls, IPS, Wireless Controler y Swicth Core la unidad de Plataformas Tecnológicas revisa la existencia de actualizaciones y cuáles son las mejoras anunciadas, luego de ello solicita a sus proveedores que generen orden de trabajo indicando el tiempo a utilizar, las ventajas y desventaja de aplicar las actualizaciones.

Respecto a la vida útil de los equipos de comunicación y seguridad de datos, se define como 8 años desde su adquisición o la fecha que el fabricante o proveedor deja de dar soporte a actualizaciones del firmware o bien al soporte de partes y piezas de Hardware de dicho equipo. Esto debe ser evaluado cada vez que la UCSC cambie de proveedor de internet (ISP), es decir cada 5 o 6 años.

2.2.5. Configuración y aplicación de políticas

La unidad de Plataformas Tecnológicas es la encargada de definir y aplicar las políticas globales de seguridad de la red institucional, como por ejemplo las restricciones y permisos de navegación de los distintos segmentos que componen la red institucional (segmento alumnos, segmento administrativos, segmento docentes).

Cada vez que uno de estos segmentos requiera un permiso de tráfico que no esté considerado o este restringido, se debe solicitar la autorización a la Dirección de Servicios Informáticos, quien evaluará la pertinencia y riegos de aplicar una regla especial en el Firewall institucional.

2.2.6. Backups

A modo de minimizar los tiempos de pérdidas de disponibilidad de la red de datos por causa de fallas de equipos o reemplazos de los mismos, la unidad de Plataformas Tecnológicas mantiene Backup actualizados de todos los equipos activos de la red, los que están alojados en el FTP Interno administrado por la unidad de Plataformas Tecnológicas. (Respaldados en procesos de Backup automatizados del storage).

2.2.7. Escalamiento y consultoría a Parthner tecnológicos

Con la finalidad de mantener operativa la red de datos la unidad de Plataformas Tecnológicas cuenta con consultoría y escalamiento de problemas a parther tecnológicos que le permiten solucionar y/o realizar tareas más complejas en la red institucional

[1] Switch layer2: equipos de comunicación que tiene la capacidad de segmentar la red en distintas redes virtuales (VLAN).
[2] Switch layer 3: equipos de comunicación que tienen la capacidad de segmentar la red en distintas redes virtuales (VLAN) y controlar o rutear el tráfico entre VLAN.

3. Estándares de seguridad para la plataforma tecnológica

La unidad de Plataformas Tecnológicas es la responsable de mantener operativa la plataforma de servidores de aplicaciones y servicios institucionales, define las medidas para resguardar la seguridad y correcta operación de los mismos.

3.1. Identificación de la plataforma tecnológica

La unidad de plataformas tecnológicas, ha identificado un conjunto de equipos, servicios y tecnologías asociadas a los cuales es necesario definir y aplicar estándares o políticas de seguridad, estos son:

- Servidores institucionales
- Sistemas Operativos
- Bases de Datos
- Correo institucional
- Servicio DNS Institucional
- Servicio Web
- Monitoreo de la plataforma
- Red de datos, segmento de servidores
- Respaldos institucional

3.2. Definición de estándares de seguridad de la plataforma tecnológica

La unidad de Plataformas Tecnológicas ha establecido un conjunto de medidas que otorgan seguridad a la plataforma informática, a saber:

3.2.1. Sala de Servidores Institucionales o Data Center

La sala de servidores institucionales debe cumplir con los siguientes estándares:

- Aire Acondicionado que mantenga una temperatura adecuada.
- Estabilizador de corriente (UPS), que regule la corriente entrante a los servidores y permita la activación automática de la red de energía de emergencia (equipo electrógeno)
- Equipo electrógeno que permita entregar energía eléctrica en el caso de falla de la red tradicional.
- Acceso restringido y controlado a sala de servidores.
- Cámara de seguridad que registre los movimientos realizados en la sala.
- Sistema de extinción de fuego.

3.2.2. Servidores Institucionales

Los servidores institucionales deben cumplir con los siguientes estándares:

- Ordenamiento de Servidores por criticidad y uso:
    - Servidores en explotación con servicios críticos
    - Servidores en explotación con servicios no críticos

- Servidores de desarrollo
- Servidores testing/contingencias.

- Obsolescencia Tecnológica de Servidores:
  - Servidores en explotación con servicios críticos[3]: está determinada por el tiempo de soporte y garantía de hardware que entrega el proveedor. Actualmente el proveedor es DELL y entrega 3 años de soporte y garantía, extensible por dos años más. Tiempo máximo de uso 5 años.
  - Servidores en explotación con servicio no críticos, testing y contingencias y servidores de desarrollo: está determinada por la capacidad de uso y buenas condiciones que presenta el servidor para entregar los servicios requeridos. Tiempo máximo de uso 8 años.

3.2.3. Sistemas Operativos

Todos los sistemas operativos que se utilicen en los servidores institucionales deben contar con los siguientes estándares:

- Capacidad de actualización, es decir que el proveedor del sistema operativo entregue soporte formal (Ej. parches y/o actualizaciones ya se para superar problemas críticos de seguridad o mejorar la aplicación.)
- El personal de Plataformas Tecnológicas debe realizar actualizaciones, a los Sistemas Operativos de los servidores, con periodicidad máxima de un año, desde algún repositorio oficial de la marca del sistema operativo.
- Llevar registro en la bitácora de operaciones de las actualizaciones realizadas a los sistemas operativos.
- El sistema operativo desde contar con soporte externo, ya sea permanente o por eventualidad ocurrida.
- Las claves del administrador deben tener un largo mayor o igual a 8 caracteres y debe ser cambiada como mínimo una vez cada 2 años. Estas claves de acceso deben ser almacenadas en un archivo Excel y subidas al servidor FTP "intranet.ucsc.cl", la ubicación y permisos de acceso del archivo será permitido sólo para el Director de la DSI y Jefe de Plataformas Tecnológicas.
- Permitir la incorporación al sistema de monitoreo de infraestructura tecnológica (Nagios).
- Para el caso de servidores windows se debe contemplar la instalación de antivirus con capacidad de actualización.
- Contar con capacidad de acceso remoto mediante algún protocolo de acceso seguro, como ssh.
- El personal de Plataformas tecnológicas debe realizar revisiones de log, funcionalidades y seguridad al menos una vez al año.

[3] Servicio Crítico: son aquellos que generan dependencia en la operación normal de las labores de la institución y afectan fuertemente la imagen corporativa (Correo institucional, intranet, sitio web institucional, sistemas transaccionales, universidad virtual, Base de Datos)

3.2.4. Bases de Datos

Las bases de datos institucionales deben cumplir con los siguientes estándares:

- Capacidad de actualización, es decir que el proveedor de Base de Datos entregue parches y/o actualizaciones ya se para superar problemas críticos de seguridad o mejorar el desempeño del software.
- La plataforma de Base de Datos debe contar con soporte externo, ya sea parmente o por eventualidad ocurrida
- Las claves del administrador deben tener un largo mayor o igual a 8 caracteres y debe ser cambiada como mínimo una vez cada 2 años. Estas claves de acceso deben ser almacenadas en un archivo Excel y subidas al servidor FTP "intranet.ucsc.cl", la ubicación y permisos de acceso del archivo será permitido sólo para el Director de la DSI y Jefe de Plataformas Tecnológicas.
- Permitir la incorporación al sistema de monitoreo de infraestructura tecnológica (Nagios).
- Contar con capacidad de acceso remoto mediante algún protocolo de acceso seguro, como ssh.
- El personal de Plataformas tecnológicas debe realizar revisiones de log, funcionalidades y seguridad al menos una vez al año
- Las BD de los sistemas institucionales (académico, administrativo financiero, fondo de crédito, personal) deben contar con respaldado logico y en un medio físico. Lo respaldos lógicos deben ser diarios y una vez a la semana generar respaldos en medios físicos extraíbles.
- Los respaldos institucionales, tanto lógicos como físicos, deben mantenerse físicamente en un lugar protegido y fuera de las instalaciones de la DSI.

3.2.5. Correo Electrónico

El correo electrónico institucional debe cumplir con los siguientes estándares:

- Capacidad de actualización, es decir que el proveedor de la plataforma de correo entregue parches y/o actualizaciones ya se para superar problemas críticos de seguridad o mejorar la aplicación
- La plataforma de correo institucional debe contar con soporte externo, ya sea permanente o por eventualidad ocurrida
- Las claves del administrador deben tener un largo mayor o igual a 8 caracteres y debe ser cambiada como mínimo una vez cada 2 años. Estas claves de acceso deben ser almacenadas en un archivo Excel y subidas al servidor FTP "intranet.ucsc.cl", la ubicación y permisos de acceso del archivo será permitido sólo para el Director de la DSI y Jefe de Plataformas Tecnológicas.
- Permitir la incorporación al sistema de monitoreo de infraestructura tecnológica (Nagios).
- Contar con capacidad de acceso remoto mediante algún protocolo de acceso seguro, como ssh.
- El personal de Plataformas tecnológicas debe realizar revisiones de log, funcionalidades seguridad al menos una vez al año
- Tener habilitado el SMTP Autenticado.

- Contar con antivirus que revise y detenga el envío de virus a través de correos electrónicos.
- Contar con anti spam que disminuya el ingreso de correo no deseado (spam) a las casillas de la universidad.
- Se debe contar con políticas informadas respecto a la responsabilidad del uso de las cuentas de correo institucionales.
- Se debe contar con políticas informadas respecto a la seguridad de claves.

3.2.6. Red de datos, segmento de servidores

El segmento de red de servidores es administrado por la unidad Soporte Tecnológico, Redes y Comunicación de datos y deben cumplir los siguientes estándares:

- Los servidores deben estar protegidos por un Firewall/Ips, que permita bloquear el acceso no permitido, entregando acceso solo por los puertos de comunicación que esten abiertos y correspondan al servicio entregado.
- Los servidores de acceso más público y masivo, como los servidores de correo electrónico, servidores web, servidores ftp, servidores dns y servidores de aplicaciones, deben estar ubicados en la zona del firewall denominada como DMZ (zona desmilitarizada).
- Los servidores que requieran un mayor grado de seguridad y control, como los servidores de bases de datos, servidores de respaldo, deben estar ubicados en las zonas seguras (Trust) del firewall.

3.2.7. Respaldo Institucional

Para el sistema de respaldo institucional se debe cumplir el siguiente estándar:

- Los respaldos generales de bases de datos y aplicaciones deben contar con respaldo en un medio físico extraíble.
- Las BD de los sistemas institucionales (académico, administrativo financiero, fondo de crédito, personal) deben contar con respaldado lógico y en un medio físico. Lo respaldos lógicos deben ser diarios y una vez a la semana generar respaldos en medios físicos extraíbles.
- Las aplicaciones institucionales deben ser respaldas en medios físicos una vez a la semana.
- Los respaldos institucionales, tanto lógicos como físicos, deben mantenerse físicamente en un lugar protegido y fuera de las instalaciones de la DSI.
- Debe realizarse la verificación de la correcta ejecución del proceso de respaldo cada vez que este sea efectuado.
- En caso de fallas del proceso de respaldo, debe volver a ejecutarse generar el análisis de las causas, así como las medidas correctivas y/o preventivas necesarias.
- Debe existir un reporte de respaldos y una bitácora para las pruebas de respaldo.
- La información institucional debe permanecer en medios de respaldo un período de 15 años. En todo caso la eliminación deberá pasar por la aprobación de todos los estamentos involucrados.

UNIVERSIDAD CATOLICA DE LA SANTISIMA CONCEPCION
Dirección de Servicios Informáticos

4. Estándares de seguridad para aplicaciones informáticas institucionales

Las unidades de Desarrollo y Soporte de Sistemas Institucionales son los responsables de brindar el apoyo a la institución mediante la implementación, implantación, mantención y soporte de aplicaciones informáticas aplicaciones institucionales, definiendo además los estándares para el desarrollo seguro de aplicaciones.

4.1. Identificación de tipos de aplicaciones

Las unidades de Desarrollo y Soporte de Sistemas Institucionales definen los siguientes tipos de aplicaciones:

- Aplicaciones Web: aplicaciones construidas en forma interna para ser utilizadas por la intranet institucional o a través de internet
- Aplicaciones en general: aplicaciones construidas en ambiente cliente- servidor.

4.2. Definición de estándares de seguridad para aplicaciones institucionales

Las unidades encargadas del soporte, mantención y desarrollo de las aplicaciones institucionales deben cumplir con los siguientes estándares en los desarrollos que realicen en pos de fortalecer la seguridad de las aplicaciones que están bajo su responsabilidad:

4.2.1. Aplicaciones Web

- Todas las aplicaciones Web que se desarrollan deben tener un encabezado de seguridad que no permita el ingreso a la página, por un medio distinto a la Intranet, es decir: control de sesión mediante autentificación de usuario, control de despliegue de páginas web y control de tiempo de sesión.
- El ingreso a las aplicaciones web institucionales debe está restringido por roles.
- Caducación de roles en la intranet de manera automática al cambiar el estado de los usuarios. Ejemplo: para el caso de funcionarios, al caducar su contrato se caduca en forma automática el Rol Funcionario de la Intranet y para el caso de alumnos, al cambiar el estado de su plan a "Eliminado", o "Renunciado" el Rol de Alumno caduca automáticamente. En el caso que el nuevo estado sea "Titulado", el Rol de Alumno caduca y se genera el Rol de Ex alumno.
- Cada desarrollo debe contemplar que la aplicación sólo pueda ser ejecutada para los roles permitidos, no se pueden postear datos de relevancia que vulneren la seguridad de la información.

4.2.2. Aplicaciones en general

- Todas las aplicaciones deben contemplar acceso mediante login y password.
- Las claves de acceso deben ser alfanuméricas de 6 caracteres como mínimo.
- El crear y/o bloquear cuentas de Base de datos, para ingresar nuevos usuarios a los sistemas, es función solo del DBA.
- Para los sistemas cliente-servidor, se habilita cada IP a través del Firewall institucional.

- Todo desarrollo y/ o mantención de aplicaciones institucionales debe cumplir con los estándares de nomenclaturas que hace referencia el documento "Nomenclatura para el desarrollo informático".
- Todo desarrollo y/o mantención debe estar ajustado a lo establecido en el procedimiento "Diseño y Desarrollo aplicaciones institucionales.