UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

3.1 Diseño de seguridad en una organización

El enfoque técnico para el diseño de seguridad es primordial, ya que es la base en la aplicación de metodologías y procesos que ayuden o garanticen la protección de los activos.

En este enfoque se incluyen los diferentes entornos que necesitamos relevar para aplicar, posteriormente, procesos, actividades o elementos que brinden soporte y seguridad.

3.1.1 Modelos de defensa

Un modelo de defensa puede ser *customizado* por la organización, el siguiente es un ejemplo estándar:

Figura 1. Modelo de defensa

Fuente: elaboración propia.

Destacamos estos ámbitos como principales en el diseño de arquitectura para la seguridad de la información. Veamos cada uno de ellos:

Negocio: es fundamental la objetividad en el modelo de negocio de la organización que oriente y siga el lineamiento en la seguridad TI. Muchas veces es la seguridad la que debe adaptarse al modelo de negocio, ya que existen procesos riesgosos. Conocer en profundidad el modelo de negocio permitirá diagramar estratégicamente una arquitectura de seguridad que nos permita ir de la mano con los objetivos.

Para lleva a cabo este acompañamiento, podemos destacar los siguientes pasos en la administración:

Figura 2: Administración de negocio y seguridad

Fuente: elaboración propia.

Gestión de arquitectura de seguridad: este punto administra los controles que se realizan en distintos ámbitos de la organización, lo cual es importante para el desarrollo de la arquitectura final de seguridad de la información dentro de la organización.

Marco normativo: los marcos son aquellos que dan un sustento técnico en la aplicación de controles en los procesos de la organización. Existen variados tipos y en la figura 3 están los más renombrados.

Figura 3: Comparativa de marcos normativos

Concepto	ITIL (Information Tecnología Infraestructura Library)	COBit (Control Objetives for Information and related Technology	CMMI (Capability Maturty Moder Integration)	ISO 27000
Objetivo	Proporcionar a los administradores de sistemas TI las mejores herramientas y documentos que les permitan mejorar la calidad de sus servicios, es decir, mejorar la satisfacción del cliente al mismo tiempo que alcanzan los objetivos estratégicos de su organización. Para esto, el departamento de TI debe ser considerado como una serie de procesos estrechamente vinculados.	Brindad buenas prácticas a través de u marco de trabajo de dominios y procesos, y presentar las actividades de una manera manejable y lógica. Estas prácticas están enfocadas más al control que a la ejecución.	Evaluar la madurez de los procesos de una organización y proporcionar una orientación referente a cómo mejorar los procesos que darán lugar a mejores productos.	Definir requisitos para un Sistema de Gestión de seguridad de la información (SGSI), para garantizar controles de seguridad adecuados para proteger la información.
Fases o etapas	Ciclo de vida del servicio: 1- Estrategia del servicio 2-Diseño del servicio 3- Transición del servicio 4- Operación del servicio 5- Mejora continua del servicio	**Dominio**: agrupación de procesos o responsabilidad organizacional. **Procesos**: conjunto de actividades unidas por delimitaciones. **Actividades:** acciones para lograr un resultado mediable.	Se divide según su nivel de madurez empresarial: incompleto, inicial o realizado, administrado, definido, administrado cuantitativamente, optimizar.	1- Diagnóstico 2- Planificación 3- Implementación 4- Evaluación
Ventajas	1- Mejora la comunicación con clientes y usuarios finales, según puntos de comunicación acordados. 2- Los servicios se detallan en lenguaje del cliente. 3-Mejor manejo de la calidad y costos de servicio. 4- Calificación de roles. 5- Comunicación entre departamentos.	1- Se aprecian resultados en indicadores de eficiencia y efectividad. 2- Permite el desarrollo de políticas claras y buenas prácticas para el control de TI en todas las organizaciones. 3- Ayuda a aumentar el valor de TI al resaltar el cumplimiento de normas.	1- Reduce costo de desarrollo. 2- Localización y resolución de defectos. 3- Mejora en la fiabilidad de la planificación, en términos de dedicación y de calendario. 4- Aumento de productividad. 5- Mejora la calidad del producto.	1- Mayor competitividad que diferencia a la organización. 2- Logro de un sistema controlado y metódico que proporciona seguridad. 3- Reducción de riesgos. 4- Mayor compromiso de mantenimiento y mejora de la seguridad. 5-Adaptación a la legislación vigente.
Desventajas	1-Tiempo y esfuerzo necesario para su implementación. 2-Dificultad de cambio empresarial. 3-Falta de comprensión en algún proceso y como deben ser controlados los errores.	1-Es un modelo ambicioso que requiere profanidad de estudio.	1- Falta de adecuación al enfoque del servicio de TI. 2-Proceso de evaluación costoso en tiempo y esfuerzo. 3-Complejidad de evaluación.	Para realizar cada una de las fases se tiene que presentar una serie de documentos que permiten que se cumplan todos los requisitos de la norma ISO 27001.
Función	Mapeo de TI. Nivel: servicio de administración.	Proceso de Mapeo de T.I.	Administración de riesgos.	Información de seguridad en Marco de referencia (Framework).
Implementación	Nivel de administración del servicio.	Información del sistema de auditoría.	Enfocado a mejorar procesos.	Cumplimiento de la seguridad estándar.

Fuente: Fuente: Elaboración propia con base en AmonDeTi, 2016.

Infraestructura de seguridad: el relevamiento e inventario de la infraestructura de la organización es fundamental para conocer la situación actual. Un buen inventario de activos nos posibilita conocer qué precauciones se deben tener y qué arquitectura de seguridad se debe generar.

3.1.2 Relevamiento físico del entorno organizacional

Como vimos en otro capítulo, el entorno físico o tangible de la organización forma parte fundamental en el planeamiento de seguridad. Para el relevamiento del mismo podemos tener en cuenta:

Tabla 1: Activos humanos (personas)

Responsabilidad	Área	Interno	Mail	…
				…
				…

Fuente: elaboración propia.

Tabla 2: Activos físicos informáticos

ID Interno	Dispositivo	Número de Serie	…
			…
			…

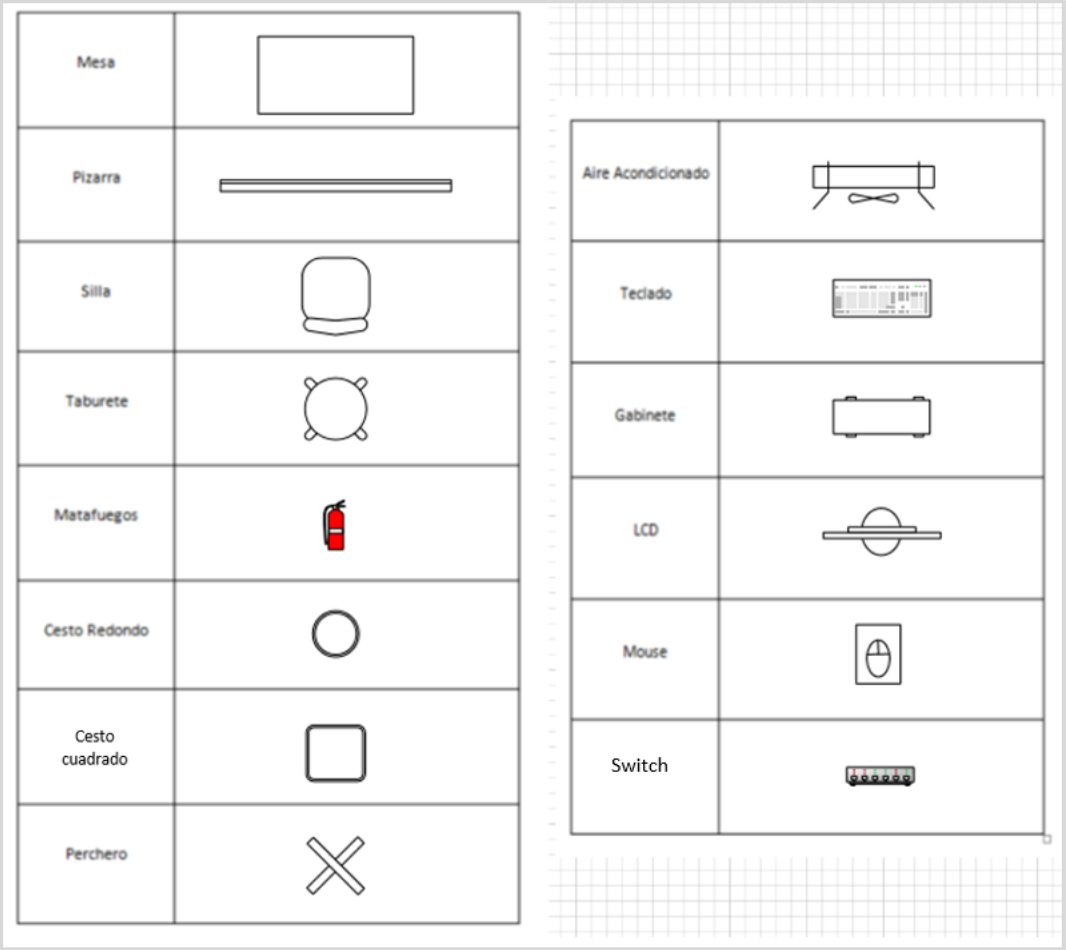
Fuente: elaboración propia.

Tabla 3: Activos físicos varios

ID Interno	Artículo	Ubicación	…
			…
			…

Fuente: elaboración propia.

Figura 4: Esquema de elementos físicos

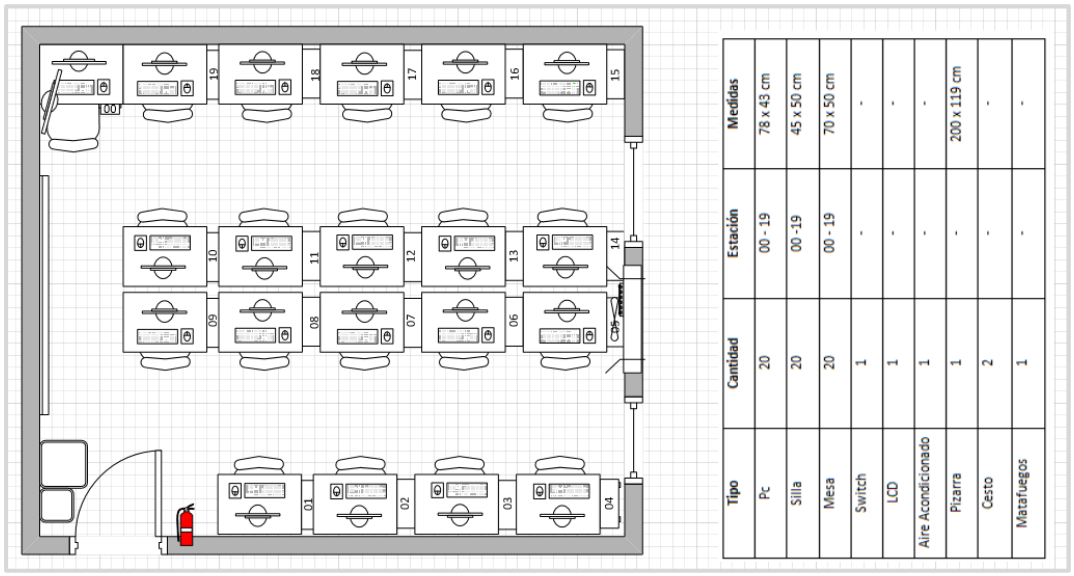


Fuente: elaboración propia.

Podemos confeccionar tablas de relevamiento que contengan los datos que la organización precise. Es fundamental generar un código interno que identifique cada uno de los activos para que, de esta forma, sean únicos. Para esto necesitaremos número de serie, modelo, marca, etc.

La generación de esquemas gráficos que muestren donde están ubicados los activos informáticos son muy útiles. Por ejemplo:

Figura 5: Esquema de un laboratorio informático



Tipo	Cantidad	Estación	Medidas
Pc	20	00 - 19	78 x 43 cm
Silla	20	00 -19	45 x 50 cm
Mesa	20	00 - 19	70 x 50 cm
Switch	1	-	-
LCD	1	-	-
Aire Acondicionado	1	-	-
Pizarra	1	-	200 x 119 cm
Cesto	2	-	-
Matafuegos	1	-	-

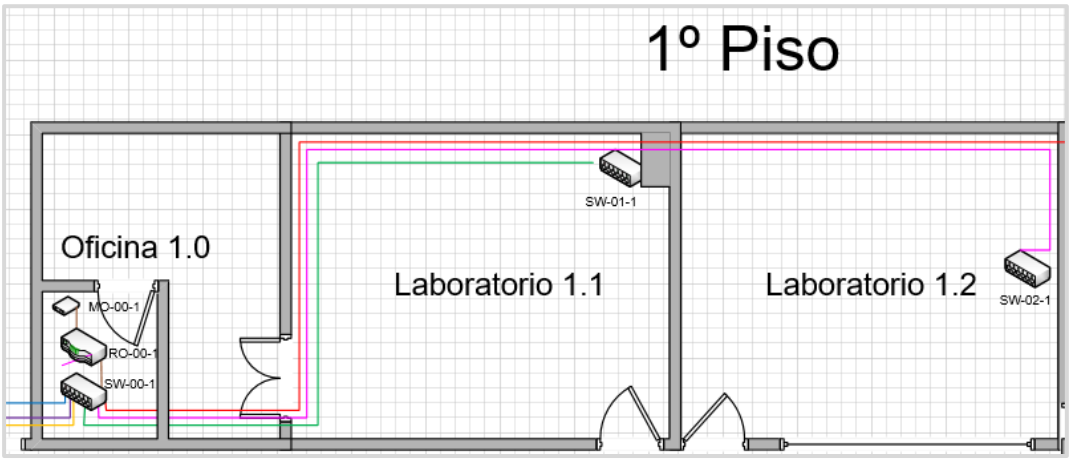
Fuente: elaboración propia.

3.1.3 Relevamiento físico del entorno de red

En el caso del entorno de red, se identifica todos los dispositivos que se encuentran en la organización. Es fundamental conocer la ubicación para poder buscarlos en casos de fallas.

Así también, se debe identificar el cableado, conocer su procedencia y dónde están conectados, para poder organizarlos. Veamos un ejemplo:

Figura 6: Esquema de red



Fuente: elaboración propia.

Figura 7: Elementos de red

Fuente: elaboración propia.

Datos a considerar en el relevamiento físico:

1) Inventario Físico
   a- Código o Número de identificación.
   b- Módulo de Rack.
   c- Marca.
   d- Tipo y Número Chasis.
   e- Marca y modelo placa madre.
   f- Marca y modelo procesador.
   g- Cantidad, Marca y modelo memoria *RAM.*
   h-Cantidad, Marca, modelo y capacidad utilizada de discos o capacidad disponible en discos.
   i- Cantidad, Marca, modelo de placas de red.
   j- Cantidad, Marca, modelo de estabilizadores o UPS.
   k- Estado.
   l- Descripción o Comentarios.
2) Inventario Lógico
   a- Sistema operativo
   b- Versión
   c- Fecha instalación
   d- Actualización.
   e- Rol / Máquina Virtual
   f- Descripción o Comentarios.
3) Otros
   a- Ubicación física de servidores.
   b- Cantidad de servidores.
   c- Diagrama eléctrico.
   d- Contención contra catástrofes.

3.1.4 Relevamiento lógico de red

Una vez reconocido y elaborado el esquema mapa de red, podemos revisar cuáles son los programas que se utilizan para la gestión de las redes, así como servidores, productos de distribución de red, seguridad de red, etc.

Se debe destacar en este análisis y esquema lógico:

- Aplicaciones en uso
  - Tipo de aplicación
  - Función
- Focalizar la centralización de datos:
  - Dónde se gestionan los datos principales
  - Por donde se encuentra el banco o generación de datos
- Representar un mapa donde se ubique cada elemento lógico

Mapa de red

Algunos lineamientos a considerar en el relevamiento:

1) Identificar redes: DMZ, VLANs, Red Datacentes, MPLS, TLS, Radio enlaces.
2) Tipo y tipología:
   a) Red de comunicaciones DC.
   b) Red de seguridad.
   c) Red de accesos VPN.
   d) Balanceadores de carga.
3) Edificio:
   a) Enrutador o puente.
   b) Switches de piso.
   c) Wi-Fi.
4) Conectividad:
   a) NAC
   b) Videoconferencia
   c) VolP
5) Segmentación de red; subredes y configuración de IP.
6) Conexiones al exterior o tercerizadas.
7) Descripción de equipamiento y dispositivos de telecomunicaciones.

3.2 Diseño de seguridad de datos

La información es el activo más importante que tiene la organización y para protegerlo encontraremos varios escalafones que precisan tanto del control humano, como el lógico (aplicaciones) dedicados a esta tarea.

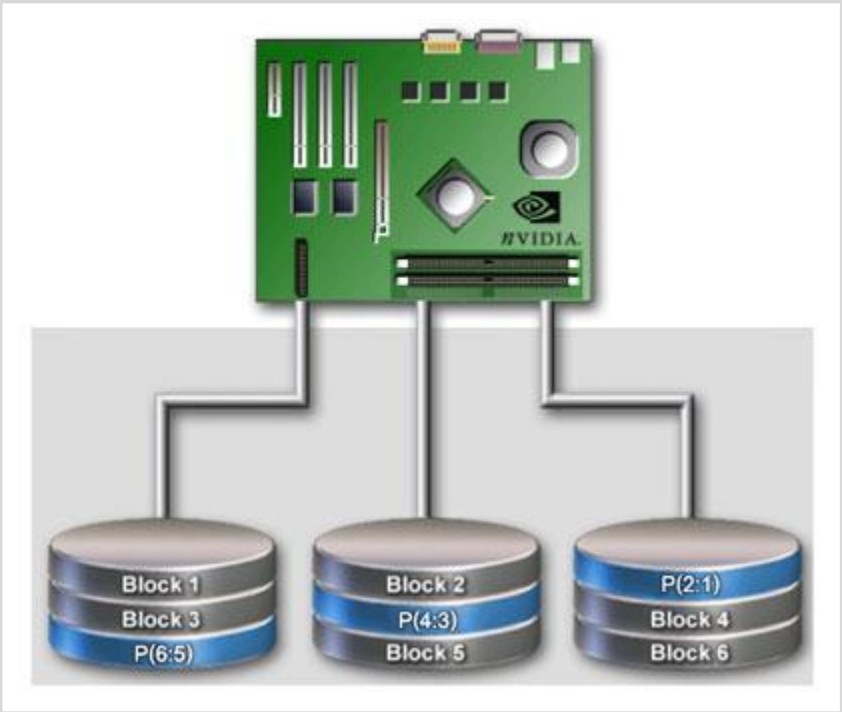
3.2.1 Protección de bases de datos

Debemos determinar el fin de la base de datos en primera instancia. Cuál es su rol o su uso; analizar el tipo de sistema operativo que ejecuta; las aplicaciones que tiene instaladas; si posee un servidor dedicado, registrar la marca y las características de *hardware*, etc. Todo esto debe estar reflejado en el inventario de activos.

Ahora bien, la protección puede ser lógica o física. Respecto a la primera, podemos destacar:

- Autorización: un usuario legítimo que puede tener acceso.
- Autenticación: validación de dicho usuario.
- Accesos:
  - DAC: accesos discrecionales.
  - MAC: políticas a nivel del sistema que no pueden ser modificadas por usuarios.
- Cifrado: aplicaciones propias o tercerizadas para realizar cifrado de datos en el respaldo de información, o almacenamiento activo del servidor.
- Parte lógica y física
- Copias de seguridad:
  - Aplicaciones dentro de los servidores que emplean procesos de respaldo de información.
  - *Hardware* que realiza constantemente o periódicamente respaldo en dispositivos físicos o en la nube.

Figura 8: Ejemplo de respaldo por *hardware*

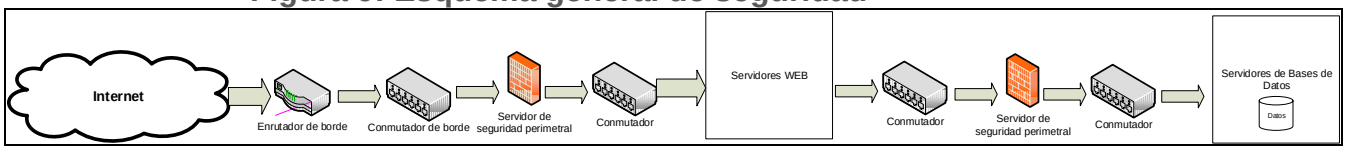


Fuente: Nvidia Corporation, 2018, recuperado de http://la.nvidia.com/object/feature_raid_es.html

Frecuentemente encontraremos recomendaciones como:

- Limitar el acceso a usuarios.
- No tener muchos administradores.
- Establecer políticas de respaldo de información.
- Controlar los accesos y reportes.
- Brindar seguridad a los periféricos de hardware.
- Brindar seguridad al acceso de *software* de base de datos.

Figura 9: Esquema general de seguridad



Fuente: elaboración propia.

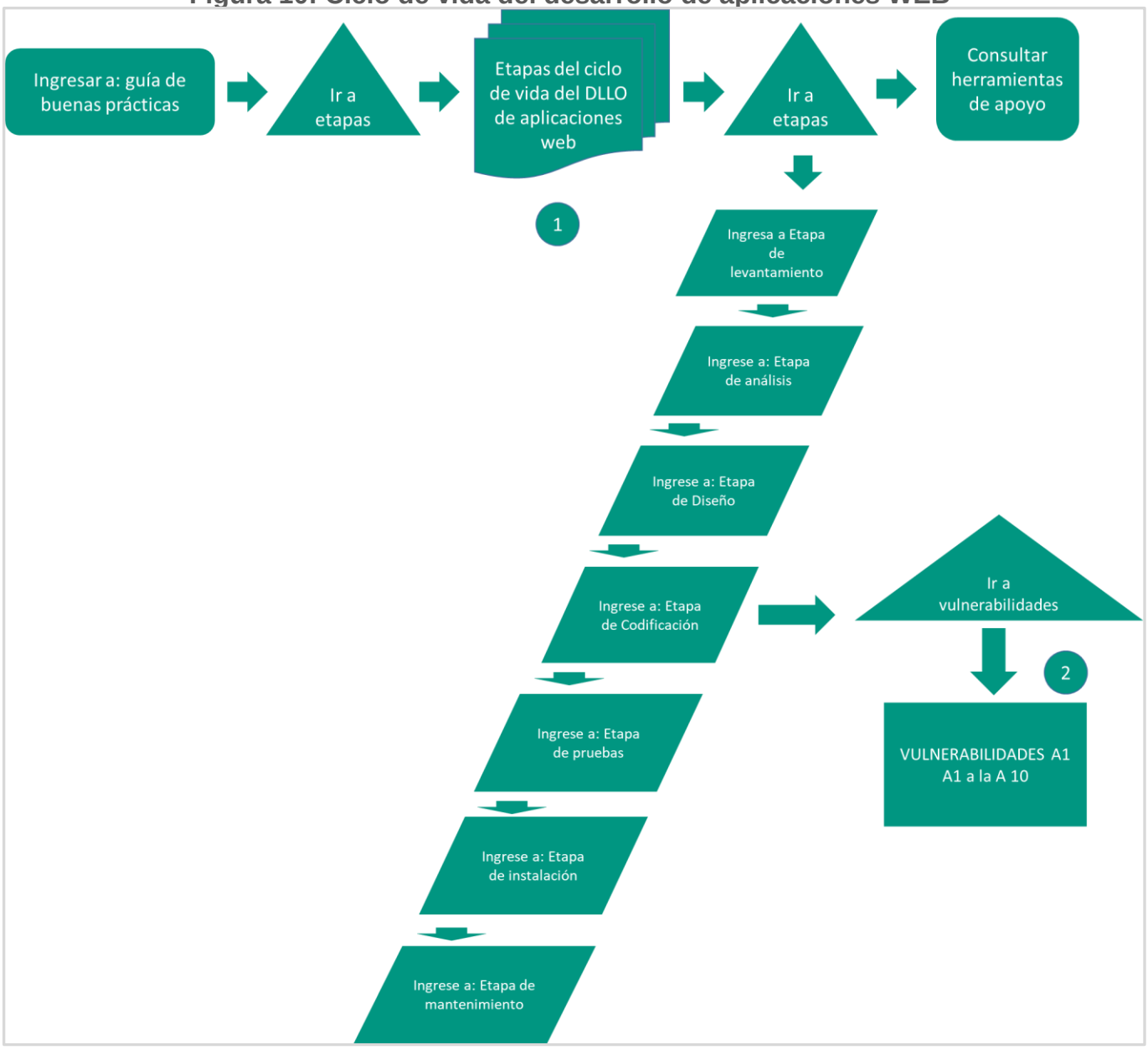
3.2.2 Protección de aplicaciones

Las aplicaciones pueden ser vulnerables en su desarrollo o cuando recién se insertan en producción. Esto quiere decir, cuando se

integran en los procesos de negocio y comienzan a utilizarlo las personas.
Para proteger aplicaciones en su estado de desarrollo podemos implementar varios modelos. Existe una guía de buenas prácticas, llamadas también OWASP, que podemos revisar en su sitio web www.owasp.org.

El desarrollo de las aplicaciones se divide en etapas que se deberían llevar a cabo con un control adecuado.

Figura 10: Ciclo de vida del desarrollo de aplicaciones WEB

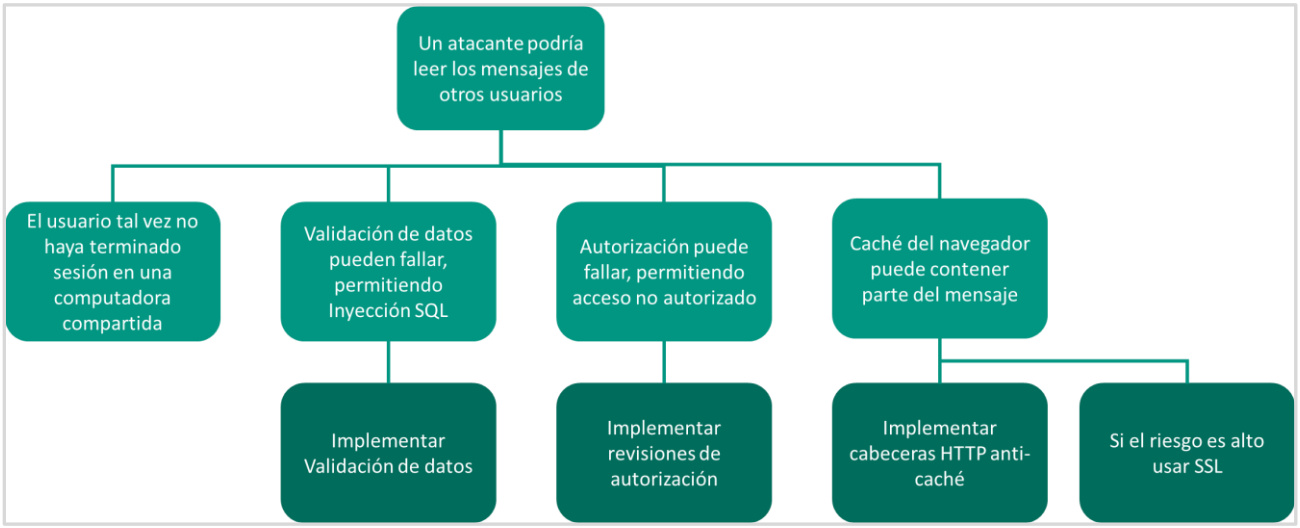


Fuente: Cújar Bahamón, 2015, recuperado de https://liliseguridadinformatica.webnode.es/guia-de-buenas-practicas/

Como podemos observar, el desarrollo de aplicaciones debería tener un ciclo en el que se incluyan precauciones para su protección antes de ponerla en funcionamiento.

Las aplicaciones web pueden ser vulnerables a los ataques en línea. Para protegerlas podemos basarnos en las buenas prácticas de OWASP.

Figura 11: Ejemplo de OWASP en proceso de ataque a aplicación



Fuente: The Open Web Application Security Project, 2002, recuperado de https://www.owasp.org/images/b/b2/OWASP_Development_Guide_2.0.1_Spanish.pdf

Un documento muy útil es el TOP 10 de OWASP que contiene los recaudos pertinentes. Podemos encontrarlo en su sitio web y utilizarlo al momento de implementar aplicaciones.

Figura 12. Tabla de análisis de riesgos (TOP 10 de OWASP)

RISK	Threat Agents	Attack Vectors: Exploitability	Security Weakness: Prevalence	Security Weakness: Detectability	Impacts: Technical	Impacts: Business	Score
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Fuente: The OWASP Foundation, 2003, p. 22.

3.2.3 Protección de computadoras

Las buenas prácticas para la protección de computadoras son variadas y generalmente apelan al sentido común de los usuarios. Pero no todas las personas son tan precavidas. En definitiva, todos tienen características diferentes y por eso pueden representar un riesgo para la organización.

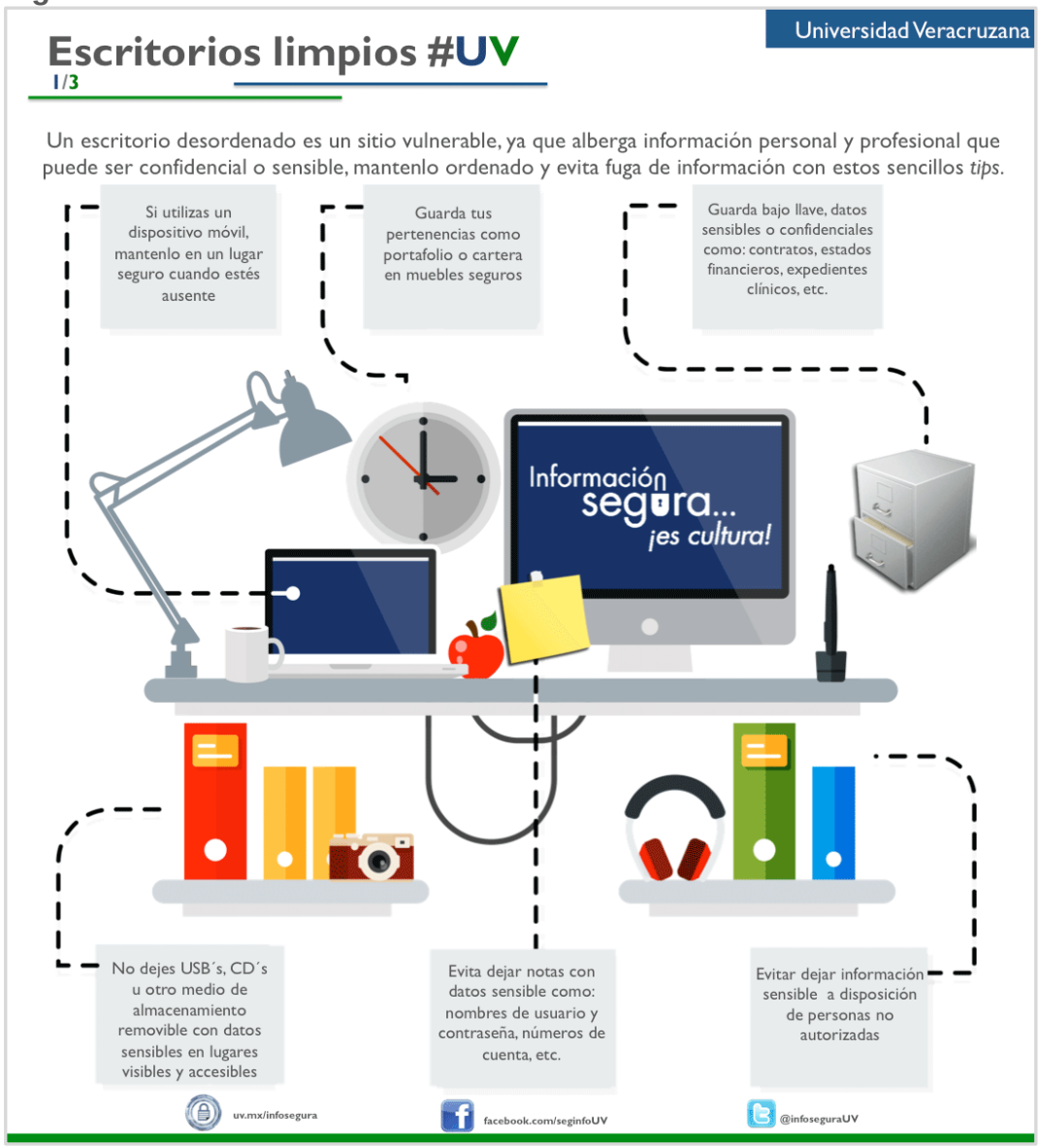
Empecemos por cuestiones simples en la protección de datos:

- *Clean desk*
  - Mantener ordenada la mesa de la computadora.
  - No dejar papeles con información sensible.
  - No pegar claves o usuarios en los monitores.
- No dejar dispositivos de almacenamiento
  - Debería tener bloqueado el uso de conexión de dispositivos, a menos que la organización no aplique esta política de seguridad.
- Bloquear el usuario si se abandona la estación de trabajo.
- Recomendar el uso de contraseñas fuertes.
- No compartir contraseñas.
- No acceder a páginas web indebidas, como, por ejemplo:
  - Hacking.

- Pornografía.
- Descarga de *software.*
- *Torrents*.

- Chequear los correos electrónicos previa apertura.
- No abrir o descargar archivos dudosos. Consultar a sistemas.
- No insertar dispositivos USB sin la autorización de seguridad sistemas.

Figura 13: *Clean desk*



Fuente: Universidad Veracruzana, 2018, recuperado de https://www.uv.mx/infosegura/infografias/

3.2.4 Protección del personal

El ámbito más vulnerable de la organización es el de las personas. Tenemos que capacitarlas y concientizarlas para proteger sus intereses.

Aquí también apelamos al sentido común, pero debemos guiar o ayudar el comportamiento de los miembros de la organización. La mejor forma es establecer políticas de seguridad y difundirlas apropiadamente, sin imponerlas, pero intervenir para que todos las acepten.

Algunas cuestiones a tener en cuenta para la protección de datos (tanto en lo laboral como en lo personal):

- Datos personales:
  - El registro de nuestros datos en diferentes servicios genera una base de datos. Las personas suelen no estar al tanto de esto y lo consideran un trámite. Es importante que conozcan que, a veces, al aceptar términos de uso se comparten datos personales con empresas. Actualmente, hay leyes que evolucionaron para mantener la privacidad de dichos datos.
  - Proteger a los usuarios con contraseñas fuertes. Es muy común que las personas piensen que no tienen nada que proteger, pero existe el dicho “tu basura es mi tesoro”. Por ejemplo: hay gente que ingresa sus datos como fecha de nacimiento, sexo y dirección, creyendo que estos datos no tienen importancia, pero las fechas de nacimiento son muy utilizados para la fuerza bruta contra las contraseñas, con las direcciones se generan bases de datos que son comparadas con otros datos recolectados de la web, y se venden a gente de mercadeo telefónico. Un medio frecuente de estafa es usurpar usuarios para realizar actividades *cibercriminales*.
- Privacidad:
  - Uno debe ser responsable de lo que publica en internet. El anonimato de las personas puede perjudicar psicológicamente a los usuarios de las publicaciones, ya que existe gente que solamente se dedica a agredir en línea, denominados: “troll” o “haters”.
  - Debe ser responsable de las imágenes que publica en la web porque probablemente queden de por vida en internet.

- Ajustar las políticas de privacidad en las redes sociales, la exposición en abundancia puede ser perjudicial. Las fotos que contienen direcciones, matrículas, ubicaciones, etc. son los nuevos medios delictivos para el crimen organizado.

- Dispositivos móviles
  - Bloquear con algún medio de seguridad, por ejemplo, un patrón, pin o huella.
  - No descargar cualquier aplicación.
  - Chequear los accesos de las aplicaciones.
  - Contar con algún antimalware.
- Redes inalámbricas
  - Tener precaución en las redes inalámbricas públicas.

Figura 14: Consejos para ser un mejor internauta

Fuente: Universidad Veracruzana, 2018, recuperado de https://www.uv.mx/infosegura/infografias/

Todos estos *tips* son recomendaciones para mejorar el uso de los dispositivos electrónicos y resguardar los datos personales. Es muy difícil acostumbrar a las personas a seguir un patrón seguro, ya que prefieren la simpleza de los medios; pero mínimamente deben conocer los riesgos. Actualmente podemos encontrar exposición desmedida de medios, imágenes con datos personales, gustos, etc. Esto permite a realizar técnicas de ingeniería social o la metodología actual de recursos humanos, el *screening*.

Se debe educar a las personas para poder tener un activo con mayores precauciones. En el caso de las organizaciones, se firman las políticas de seguridad para dar a conocer las reglas a seguir para el uso de los activos dentro de las mismas.

Referencias

Cújar Bahamón, L. (2015) Guía de buenas prácticas para el desarrollo de aplicaciones web seguras, orientadas a la formación de estudiantes de la media técnica en desarrollo de software de las instituciones educativas de la ciudad de Medellín [entrada de blog] recuperado de https://liliseguridadinformatica.webnode.es/guia-de-buenas-practicas/

Guerra, E. (4 de julio de 2012) *Un servidor de seguridad perimetral* [entrada de blog] recuperado de http://sisena-evidenciasi.blogspot.com/2012/07/un-servidor-de-seguridad-perometral.html

Nvidia Corporation (2018) Almacenamiento NVIDIA® MediaShield™ [artículo en línea] recuperado de http://la.nvidia.com/object/feature_raid_es.html

The Open Web Application Security Project (2002) Una guía para construir
aplicaciones y servicios web seguros [documento en lìnea] recuperado de https://www.owasp.org/images/b/b2/OWASP_Development_Guide_2.0.1_Spanish.pdf

The OWASP Foundation (2003) *OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks* [document en línea] recuperado de https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Universidad Veracruzana (2018) *Seguridad de la información. Infografías.* Recuperado de https://www.uv.mx/infosegura/infografias/


UNIVERSIDAD
SIGLO 21
MIEMBRO DE LA RED
ILUMNO