SEGURIDAD de la INFORMACIÓN en la UGR

Responsable de Seguridad de la Información de la Universidad de Granada

Campus de Ceuta, Granada – 28 de noviembre de 2024

Una responsabilidad compartida

OBJETIVOS

Revisión de las cuestiones más importantes relativos a la Seguridad de Información en nuestra Universidad.

ÍNDICE DE LA SESIÓN 3

1. Seguridad de la Información

Objetivos y riesgos

InfoSec

La Seguridad de la información se compone de un conjunto de medidas preventivas y reactivas que buscan la protección de la información en relación con la:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad.

Riesgos que podemos sufrir:

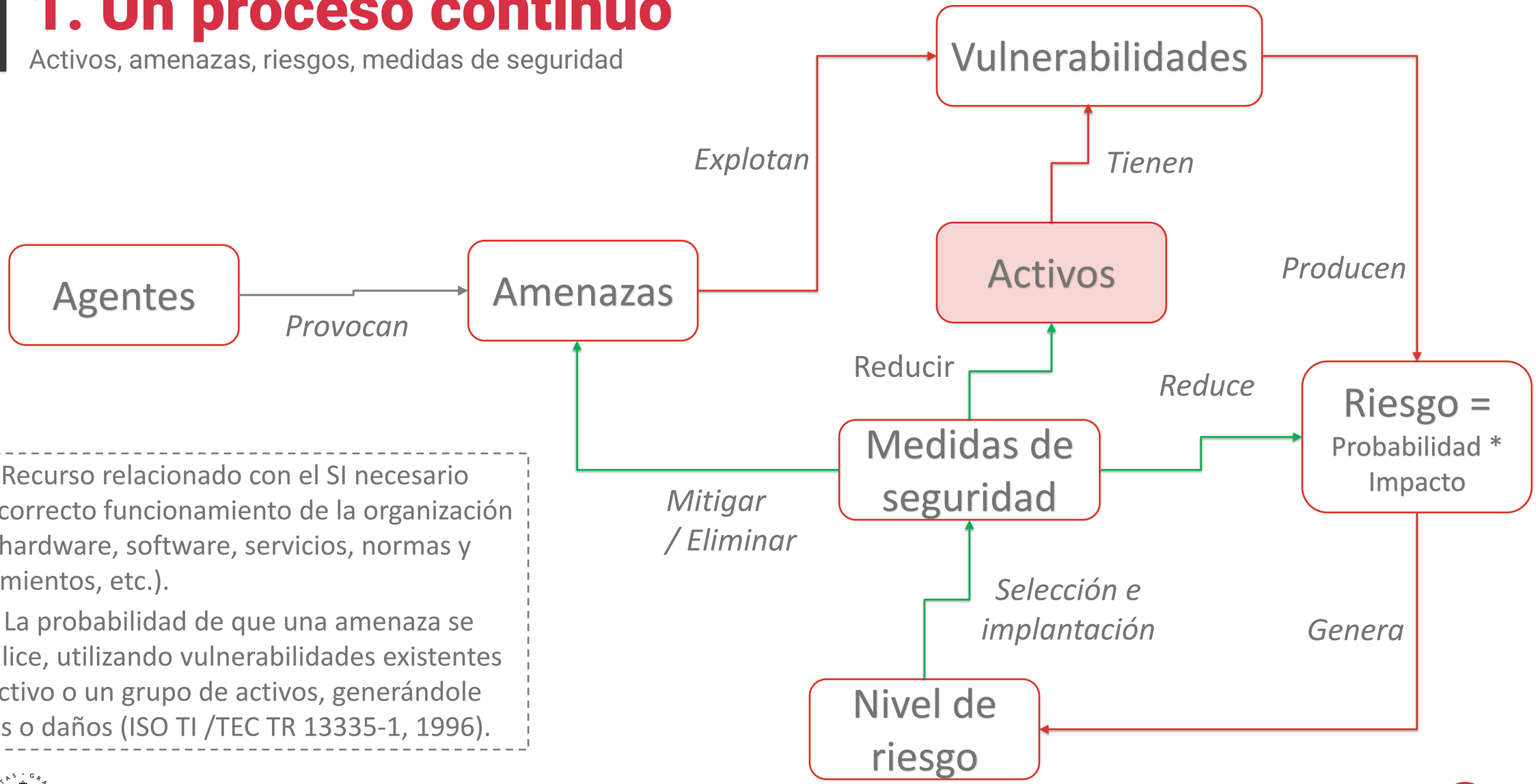
- Robo de información
- Perdidas monetarias
- Reputación
- Desventaja competitiva

...

“La seguridad no es un artilugio, es un estado mental” — Eleanor Everet

1. Un proceso continuo

Activos, amenazas, riesgos, medidas de seguridad



Activo: Recurso relacionado con el SI necesario para el correcto funcionamiento de la organización (datos, hardware, software, servicios, normas y procedimientos, etc.).

Riesgo: La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños (ISO TI /TEC TR 13335-1, 1996).

Tener siempre presente ….

Recomendación básica en nuestra relación con la información que gestionamos y almacenamos

Problema

A veces nos podemos relajar al pensar que no somos objetivo de ataques por nuestro “supuesto” escaso o nulo valor para el atacante. Un error importante, ya que debemos pensar siempre que:

¡ Nuestros activos siempre son valiosos !

(*per se* o como punto de entrada a la organización)

Monetario

Privacidad

Reputacional

Suplantación de identidad

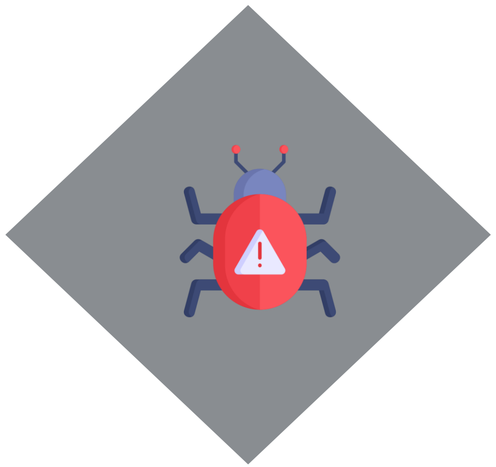
Perdida de información

1. Principales amanezas

El usuario suele ser el primer vector de ataque

Phishing

Técnica de ingeniería social destinada a engañar al destinatario de una comunicación (correo, SMS, llamada, …) a que realice la acción deseada por el atacante.



Malware

Programa malicioso diseñado para infiltrarse en un dispositivo sin el consentimiento de propietario y causar daños, interrumpir el servivio o robar datos.

Credenciales comprometidas

Credenciales en pocesión de un atacante: phishing o ing. Social, malware, fuerza bruta, deducción, mirar por encima del hombro, ...

Otras

- Exposición de terceras partes (acceso sistemas menos protegidos)
- Errores de configuración
- Pobre ciber-higiene
- Gestión de datos pobre (brechas de datos) …

2. Esquema Nacional de Seguridad (ENS)

PARA INTRODUCIR UN MENSAJE DE PRESENTACIÓN

R.D. 311/2022

> El ENS, de aplicación a todo el Sector Público, así como a los proveedores que colaboran con la Administración, ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

"Si sientes todo bajo control, es que no vas lo suficientemente rápido" — Mario Andretti

ENS en la UGR

Como institución temenos …

Política de seguridad

Aprobado en la sesión ordinaria del Consejo de Gobierno de 26 de octubre de 2022
https://secretariageneral.ugr.es/informacion/servicios/seguridad-informacion/normativa

Normas de seguridad

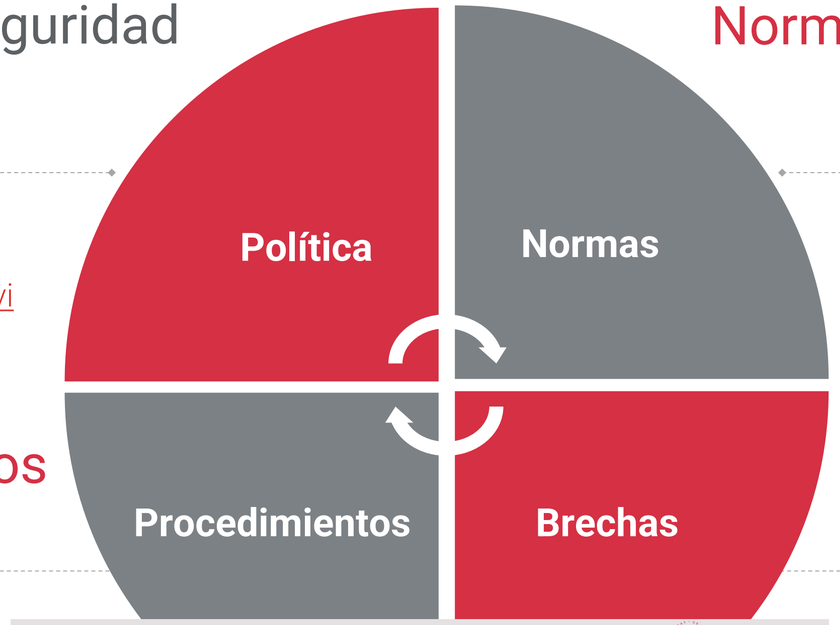
Normas de uso seguro de los recursos TIC de la UGR.
https://secretariageneral.ugr.es/informacion/servicios/seguridad-informacion/normativa

Procedimientos de seguridad

Procedimientos técnicos para la Gestión de los Sistemas de Información de la Universidad.

Incumplimientos de seguridad

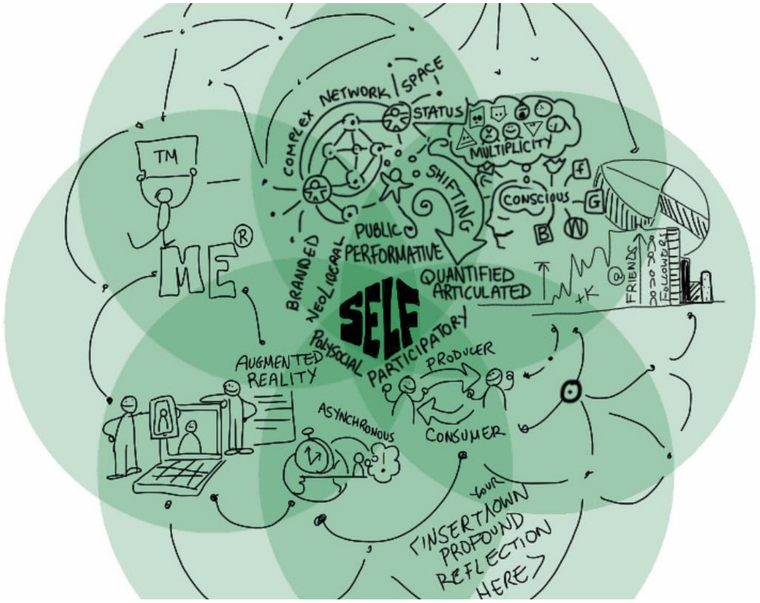
Protocolo de notificación y formulario para reportar brechas de seguridad de datos personales y medidas de protección
https://secretariageneral.ugr.es/informacion/servicios/seguridad-informacion/reportar-incidente

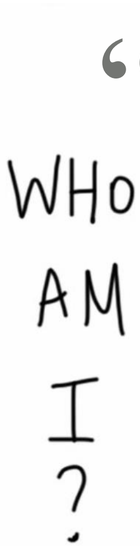


3. Identidad digital

PARA INTRODUCIR UN MENSAJE DE PRESENTACIÓN

Definiciones





Identidad digital: conjunto de información sobre una persona que se encuentra en Internet, y que le caracteriza y diferencia de los demás, como: nombre, dirección de correo electrónico, foto de perfil, comentarios, aficiones, relaciones, etc.

Una parte importante de la identidad digital es el identificador o nombre de usuario y la información de autenticación, que hace referencia a las credenciales, como las contraseñas, que se utilizan, para verificar la identidad y acceder así a los servicios en línea de manera segura.

Huella digital: al rastro que se deja en línea como resultado de las acciones en la web. Dicho de otra manera, es el registro pasivo de las actividades *online* de una persona, que puede ser utilizada por terceros para diversos fines.

"A rose is a rose is a rose" — Gertrude Stein

Identidad digital: protección

Medidas básicas para la protección de nuestra identidad digital

Algunas medidas que permiten proteger nuestra información y nuestros sistemas de información:

Problema

Usar una misma identidad digital todo el tiempo puede llegar a problemas de privacidad. Un caso:

- Cuando acciones no relacionadas son enlazadas con el propósito de predecir o controlar el comportamiento de un usuario

Contraseñas robustas

Discreción *online* y en público

Pensar antes de responder o hacer clic

Mantener las contraseñas seguras

Notificar sospechas de suplantación

3. Navegación y correos seguros

Protección en el acceso servicios de Internet a traves de navegadores y/o clientes de correo electrónico

Consideración

> Tanto la navegación web como el correo electrónico son medios básicos para el desarrollo de la labor profesional como personal.

Las estadísticas reflejan que siguen siendo los principales vectores de ataque, especialmente el correo.

“Los amateurs hackean sistemas, los profesionales hackean personas” — Bruce Shneier

Navegación segura

Proteger tu privacidad y seguridad en línea

Uso de VPN

Permite cifrar nuestra comunicación, manteniendo la privacidad y “anonimato”

Extensiones

- Bloqueadores de anuncios, de Código y de contraseñas

Opciones de privacidad y seguridad

Chrome Firefox
Safari Edge

Separación

Separar la navegación personal y laboral,

Otras recomendaciones

- Utilizar protocolos seguros
- Borrar cookies y caches
- Cuidado con las descargas

Más detalles

https://secretariageneral.ugr.es/informacion/servicios/seguridad-informacion/decalogo-ciberseguridad

Correo seguro

Cosas en las que nos debemos fijar y medidas a tener en cuenta

Referencia: INCIBE; “Consejos para hacer un uso seguro del correo corporativo“. Disponible en https://www.incibe.es/empresas/blog/consejos-hacer-uso-seguro-del-correo-corporativo

Verificar

Remitente

Verificar la identidad del remitente: nombre y dominio.

Asunto

Suele ser el gancho o reclamo.

Cuerpo

Aspecto del suplantado. Contiene una llamada a la acción (urgente).

Adjuntos / Enlaces

Nombre archivo que incita apertura. El icono suele similar un documento pero es un ejecutable / macros. URL

Medidas

Remitente

- Dominios: whois
- Cabeceras: Verlas y entenderlas

Adjuntos

- Opción para ver extension de archivos
- VirusTotal
- Deshabilitar macros

Enlaces

- VirusTotal
- Enlaces acortados: unshorten.me

Generales

Software actualizado, antimalware, filtros antispam, desactivar vistas de correo html en cuentas críticas, separar correo personal/professional, cifrado.

5. Seguridad y Teletrabajo

Elementos de seguridad a considerer durante el teletrabajo

Amenazas:

- Credenciales comprometidas
- Malware
- Filtración de datos

Mecanismos de seguridad:

- Red Privada Virtual (VPN): protege la integridad y confidencialidad.
- Infraestructura de Escritorio Virtual (VDI)

Buenas prácticas

- Actualización de software: sistemas operativo, antivirus, aplicaciones
- Verificar activación servicios seguridad: antivirus, cortafuegos
- Desconfiar en los accesos a redes públicas o abiertas
- Contraseñas fuertes
- Control de usuarios en aplicaciones colaborativas

7. Seguridad física y soportes

Controlar el acceso e integridad de nuestros dispositivos

Dos niveles:

—

- Protección hardware: integridad de los dispositivos
- Protección de datos: tránsito y almacenamiento

Protección:

—

- No dejar información a la vista
- Bloquear dispositivo
- No perder de vista nuestros dispositivo

Amenazas:

—

- Acceso Físico
- Integridad física
- Exposición de la información

...

—

- Guardar almacenamiento
- Cifrado
- Copias de seguridad

7. Seguridad en móviles y en la nube

Servicios integrados en nuestro día a día: nuevas amenazas, nuevas necesidades

Amenazas en móviles

- Filtración de datos
- Redes inseguras o inactivas (WiFi, Bluetooth,..)
- *Phishing*
- *Spyware, …*

Amenazas en la nube

- Brechas de datos
- Gestión de identidad / robo de cuentas,
- Configuraciones inseguras,
- Cumplimiento normativo, ….

Protección

- Cifrado
- Minimizar datos almacenados
- Desactivar Comunicaciones inactivas
- Verificar la instalación de apps
- Antivirus

Protección

- Visibilidad de datos: quién accede, compartición, ubicación, etc.
- Control de datos: clasificación de los datos**, cifrado seguro**, …
- Acceso a datos: controles de acceso de usuarios (2AF), dispositvos, …
- Cumplimiento normativo

8. Brechas de seguridad

Obligatoriedad de notificar las brechas de seguridad en un plazo de 72 horas

Una brecha de seguridad es un incidente de seguridad que afecta a los datos personales que maneja una empresa, tanto de clientes y proveedores como de sus propios trabajadores. El incidente puede ser accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personal.

Protocolo

https://secretariageneral.ugr.es/sites/webugr/secretariageneral/public/inline-files/UGR.-PROTOCOLO-NOTIFICACIO%C2%B4N-BRECHAS-DE-SEGURIDAD-DATOS-PERSONALES.pdf

UNIVERSIDAD DE GRANADA

FORMULARIO PARA NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Denunciante o notificante.-

DNI: Nombre y apellidos:

Teléfono de contacto: Email:

Unidad/Servicio/Dpto./Facultad/Escuela:

- Información temporal de la brecha:
  - Fecha de detección de la brecha:
  - Medios de detección de la brecha :
- Resumen del incidente:

Brecha de confidencialidad (acceso no autorizado)

Brecha de integridad (modificación no autorizada)

Brecha de disponibilidad (desaparición o pérdida)

Medidas de protección

https://secretariageneral.ugr.es/sites/webugr/secretariageneral/public/inline-files/Documento-sobre-medidas-de-proteccion.pdf

Formulario de notificación

https://secretariageneral.ugr.es/sites/webugr/secretariageneral/public/inline-files/FORMULARIO-PARA-NOTIFICACIO%CC%81N-DE-BRECHAS-DE-SEGURIDAD1.docx

GRACIAS POR SU ATENCIÓN

Para contactar a través:

Responsable de Seguridad de la Información

responsablesi@ugr.es
+34 958 24 05 72

Otras vías:

Seguridad Informática (CSIRC)

seguridadinformatica@ugr.es

CAU

csirc@ugr.es
36000 (958 241010 extensión 3, desde fuera de la UGR)