

Esquema Nacional de Seguridad

LA SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD



Fundación General
Universidad Complutense de Madrid

Índice

1. ¿Por qué?
2. Esquema Nacional de Seguridad
3. Roles y Responsabilidades
4. Órganos de referencia
5. Estado actual de la Fundación General de la Universidad Complutense de Madrid
6. Buenas prácticas en seguridad de la información
7. Dudas y consultas

Índice



1. **¿Por qué?**
2. Esquema Nacional de Seguridad
3. Roles y Responsabilidades
4. Órganos de referencia
5. Estado actual de la Fundación General de la Universidad Complutense de Madrid
6. Buenas prácticas en seguridad de la información
7. Dudas y consultas

¿Por qué?

¿Porqué necesito aprender sobre Seguridad de la Información y Ciberseguridad y aplicarla en toda la organización?

¿No es esto un problema de los informáticos?



Todo el que usa un ordenador necesita saber
cómo mantener sus datos seguros

¿Por qué?

ELMUNDO

España es el país con más ataques informáticos a través de la función de escritorio remoto

En 2021 se produjeron más de 51.000 millones ataques a través de este protocolo, el doble de los que se produjeron en Italia, segundo país en la lista



EL PAÍS

Cataluña

QUADERN

La UOC sufre un ciberataque que bloquea su campus virtual

La Universitat Oberta de Catalunya restablece en 24 horas la actividad docente

EL PAÍS
Barcelona - 02 ENE 2022 - 21:34 CET

LA RAZÓN

Tecnología

¿Te ha tocado un iPhone 13 en Instagram? Así funciona el timo del que alerta la OSI

La Oficina de Seguridad del Internauta ha advertido de una nueva campaña de estafas que emplea el iPhone 13 como cebo y busca hacerse con los datos de la tarjeta de crédito o débito de las víctimas



¡Enhorabuena! ¡Has ganado!

¡Has ganado un iPhone 13!

1. Pulsa el botón OK para pasar a la página con los precios de envío.
2. Llena el formulario y paga el precio de envío para recibir el iPhone 13 gratis.
3. El envío se realizará en 5-7 días.

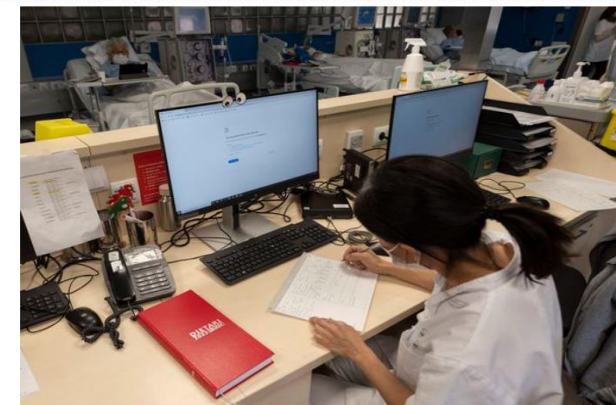
El Confidencial

Inicia

"NO PAGAREMOS NI UN CÉNTIMO"

Quién es RansomHouse, el grupo detrás del ciberataque al Hospital Clínic de Barcelona

El hospital ha sido atacado por un grupo de 'hackers' que secuestra y roba datos para pedir un rescate por ellos. Si no se paga, esa información puede acabar publicada en su web



Una sanitaria del Hospital Clínic de Barcelona trabaja tomando notas a mano este lunes después del ciberataque. (EFE/Clinic/Francisco Ávia)

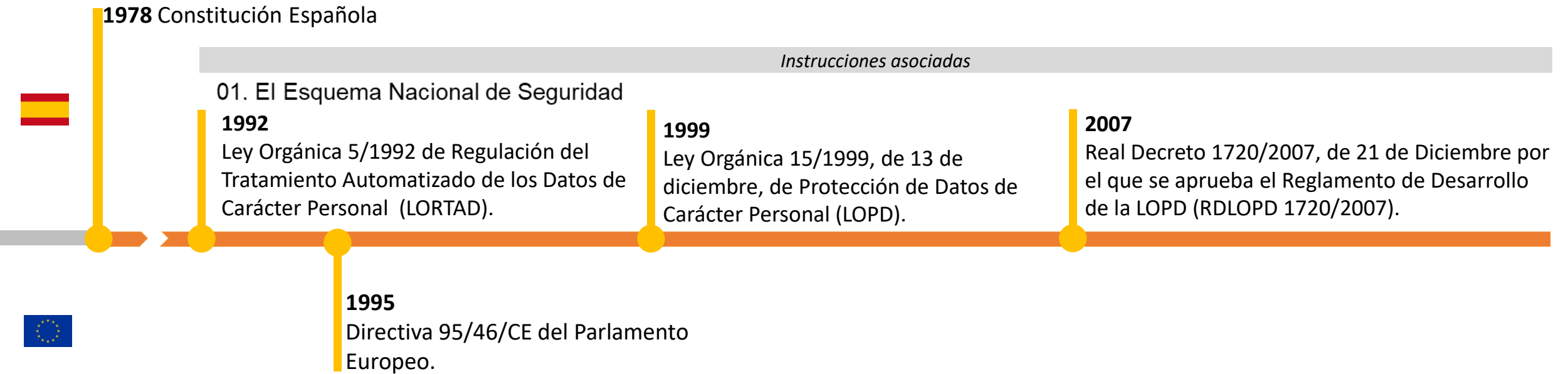
Índice



1. ¿Por qué?
2. **Esquema Nacional de Seguridad**
3. Roles y Responsabilidades
4. Órganos de referencia
5. Estado actual de la Fundación General de la Universidad Complutense de Madrid
6. Buenas prácticas en seguridad de la información
7. Dudas y consultas



Antecedentes históricos en materia de protección de datos





Nuevo ecosistema

Instrucciones asociadas

2018

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.



2019

2016

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016





Antecedentes históricos respecto Esquema Nacional de Seguridad





02. Roles y responsabilidades



RGPD. Art 32

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, **el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (...)**
2. (...)
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un **mecanismo de certificación aprobado** a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4. (...)



Aplicación del ENS

LOPDGDD. Disposición adicional primera

1. **El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse** en caso de tratamiento de datos personales (...) adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.
2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica **deberán aplicar** a los tratamientos de datos personales las medidas de seguridad que correspondan de **las previstas en el Esquema Nacional de Seguridad**, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.
3. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y **se ajustarán al Esquema Nacional de Seguridad**.



Los Esquemas Nacionales de Seguridad e Interoperabilidad: llevar a cabo los dos derechos



El **Esquema Nacional de Seguridad (ENS)** establece los principios básicos y requisitos mínimos que deben cumplir los sistemas y procedimientos, de forma que se garantice que los servicios se puedan prestar con seguridad, preservando la privacidad de los datos, y sin interrupciones. (RD 311/2022)



El **Esquema Nacional de Interoperabilidad (ENI)** establece las condiciones para que las Administraciones Públicas puedan intercambiar información, adaptando los formatos, el significado de los campos de información o los aspectos de comunicaciones. (RD 4/2010)



Requisitos mínimos

La seguridad debe desarrollarse en base a los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad
- Análisis y Gestión de riesgos
- Gestión de personal
- Profesionalidad
- Autorización y control de los accesos
- Protección de las instalaciones
- Adquisición de productos y servicios de seguridad
- Mínimo privilegio
- Integridad y actualización del sistema
- Protección de la información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registro de actividad y detección de código dañino
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad



01. El Esquema Nacional de Seguridad

Elementos

MARCO ORGANIZATIVO

Medidas relativas a la **organización global** de la seguridad



Política de seguridad



Normativa de seguridad



1 Planificación

- Análisis de riesgos.
- Arquitectura de Seguridad.
- Adquisición de nuevos componentes.
- Dimensionamiento/gestión de la capacidad.
- Componentes certificados.



4 Recursos externos

- Contratación y acuerdos de nivel de servicio.
- Gestión diaria.
- Protección de la cadena de suministro.
- Interconexión de sistemas.

MARCO OPERACIONAL

Medidas a tomar para **proteger la operación del sistema** como conjunto integral de componentes para un fin.



2 Control de acceso

- Identificación.
- Requisitos de acceso.
- Segregación de funciones y tareas.
- Proceso de gestión de derechos de acceso.
- Mecanismo de autenticación (usuarios externos).
- Mecanismo de autenticación (usuarios de la organización).



5 Servicios en la nube

- Protección de servicios en la nube.



3 Explotación

- Inventario de activos.
- Configuración de seguridad.
- Gestión de la configuración de seguridad.
- Mantenimiento y actualizaciones de seguridad.
- Gestión de cambios.



6 Continuidad del servicio.

- Análisis de impacto.
- Plan de continuidad.
- Pruebas periódicas.
- Medios alternativos.

MEDIDAS DE PROTECCIÓN

Medidas para **proteger activos concretos**, según su naturaleza, con el nivel requerido en cada dimensión de seguridad



8 Protección de la información

- Protección frente a código dañino.
- Gestión de incidentes.
- Registro de la actividad.
- Registro de la gestión de incidentes.
- Protección de claves criptográficas.



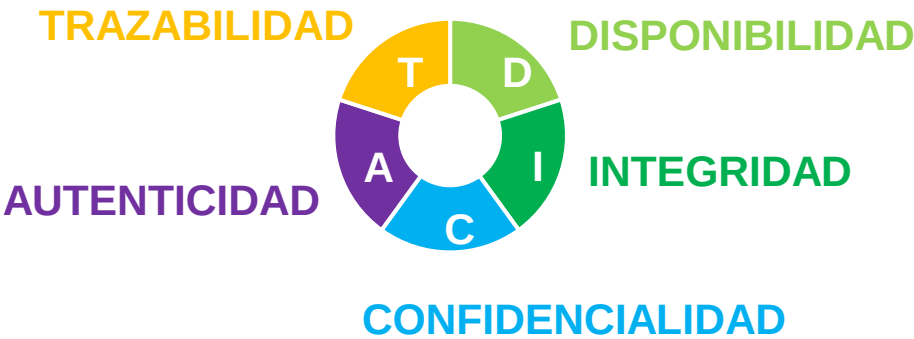
7 Monitorización del sistema.

- Detección de intrusión.
- Sistema de métricas.
- Vigilancia.



¿Qué medidas de seguridad desplegar?

Dependiendo de **cómo pueda afectar un incidente** de seguridad puede afectar **a un servicio** o información en una o más dimensiones de seguridad.



Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.acc	Control de acceso				
op.acc.1	Identificación	TA	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	CITA	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	CITA	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	CITA	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	CITA	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	CITA	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9



Análisis de Riesgos / Plan Director de Seguridad ENS

- Categoría del sistema: MEDIA

Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Medio	Medio	Medio	Medio	Medio

COD	Servicio	CATEGORÍA ENS	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
SENS_01	Gestión de la Investigación	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_02	Gestión de actividades culturales	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_03	Gestión de becas y ayudas	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_04	Gestión de actividades formativas y eventos	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_05	Portal Institucional	MEDIO	Medio	Básico	0	Básico	0
SENS_06	Portal de Transparencia	MEDIO	Medio	Medio	0	Medio	Medio
SENS_07	Actividades que contribuyan a la mejor atención a la comunidad	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_08	Pulsa	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_09	Económico-Financiera	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_10	Gestión de congresos	MEDIO	Medio	Medio	Básica	Medio	Básico
SENS_11	Relaciones Institucionales y Mecenazgo	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_12	Jurídico	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_13	Perfil del contratante	MEDIO	Medio	Medio	Básico	Medio	Medio
SENS_14	Empleo y Formación Bonificada	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_15	Recursos Humanos	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_16	Comunicación	MEDIO	Básico	Medio	0	Medio	Básico

Índice

1. ¿Por qué?
2. Esquema Nacional de Seguridad
-  3. **Roles y Responsabilidades**
4. Órganos de referencia
5. Estado actual de la Fundación General de la Universidad Complutense de Madrid
6. Buenas prácticas en seguridad de la información
7. Dudas y consultas



02. Roles y responsabilidades



- Roles del ENS
- Roles del RGPD



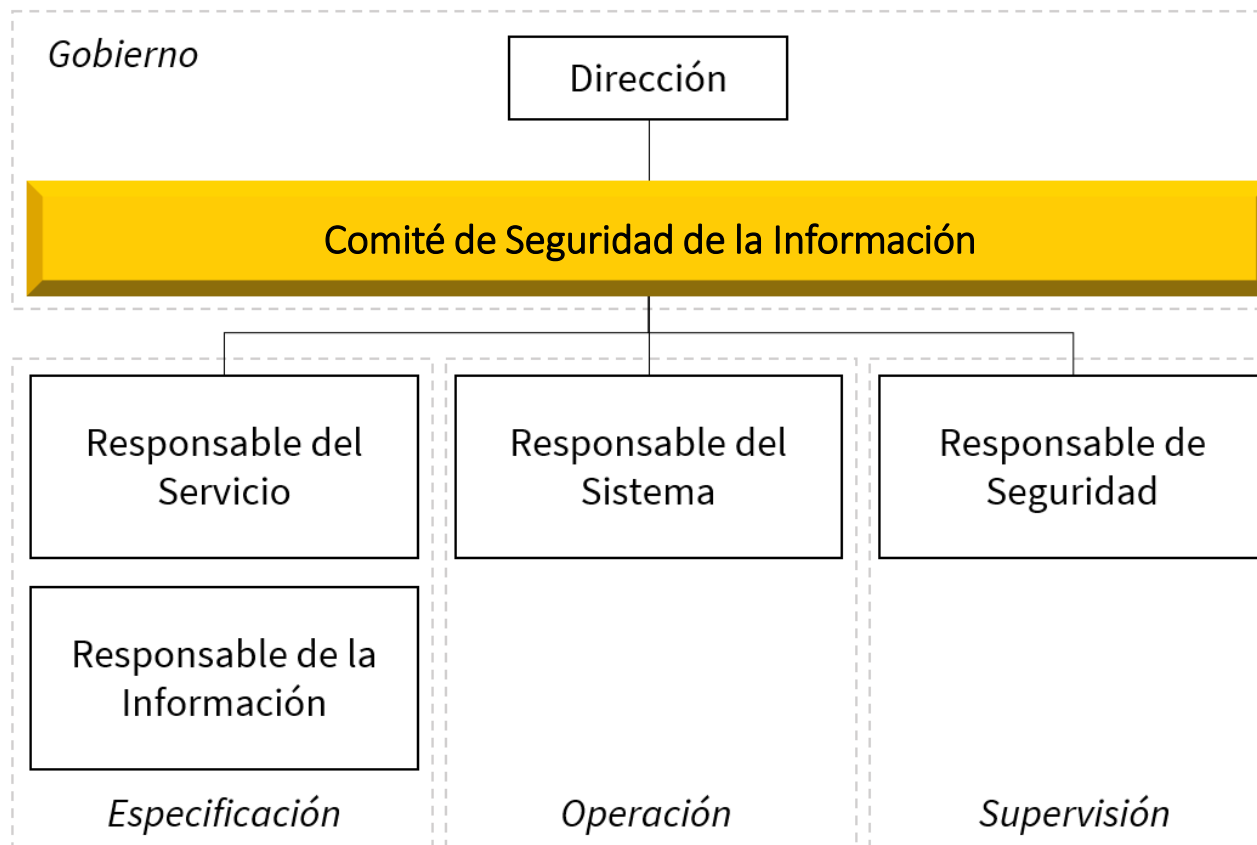
El Responsable del Tratamiento y el Responsable de la Información son figuras equivalentes en ambas normas:

- Perfil de responsabilidad máxima
- Rol de especificación

Igual ocurre con el encargado del Tratamiento y el Responsable del Sistema.



Organización de la Seguridad



Índice

1. ¿Por qué?
2. Esquema Nacional de Seguridad
3. Roles y Responsabilidades
4. **Órganos de referencia**
5. Estado actual de la Fundación General de la Universidad Complutense de Madrid
6. Buenas prácticas en seguridad de la información
7. Dudas y consultas



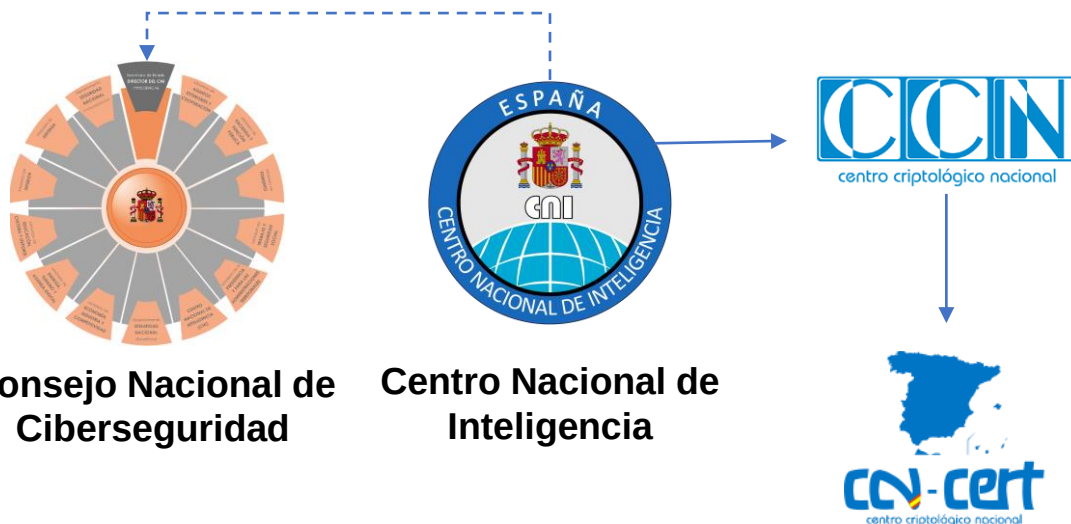


03. Órganos de referencia



Fundación General
Universidad Complutense de Madrid

Órganos de coordinación y gestión de la Seguridad TIC a nivel nacional



Consejo Nacional de
Ciberseguridad

Centro Nacional de
Inteligencia



Coordinación y respuesta a incidentes

- CCN-STIC-800 Glosario de términos
- CCN-STIC-801 Responsabilidades
- CCN-STIC-802 Auditoria
- CCN-STIC-803 Valoración de los sistemas
- CCN-STIC-804 Medidas de implantación del ENS
- CCN-STIC-805 Política de seguridad
- CCN-STIC-806 Plan de adecuación
- CCN-STIC-808 Verificación de cumplimiento de medidas
- CCN-STIC-809 Declaración de conformidad
- CCN-STIC-811 Interconexión en el Esquema Nacional de Seguridad
- CCN-STIC-812 Seguridad en Entornos y Aplicaciones Web
- CCN-STIC-815 Métricas e indicadores en el ENS
- CCN-STIC-818 Herramientas de Seguridad en el ENS
- CCN-STIC-824 Informe del Estado de la Seguridad

Órganos de coordinación y gestión de la protección de datos



- Vela por el cumplimiento de la legislación sobre protección de datos
- Controla su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
- Es **autoridad de control** a nivel nacional
- Coordinación de otras autoridades de control autonómicas
- Vela y controla el cumplimiento de la legislación sobre protección de datos en la Comunidad Autónoma de Andalucía.
- Es la **autoridad de control** en Andalucía
- Resuelve las reclamaciones presentadas por incumplimiento de la N. Protección de Datos
- Promueve la cultura de la protección de datos personales

Índice

1. ¿Por qué?
2. Esquema Nacional de Seguridad
3. Roles y Responsabilidades
4. Órganos de referencia
-  5. **Estado actual de la Fundación General de la Universidad Complutense de Madrid**
6. Buenas prácticas en seguridad de la información
7. Dudas y consultas



Fundación General

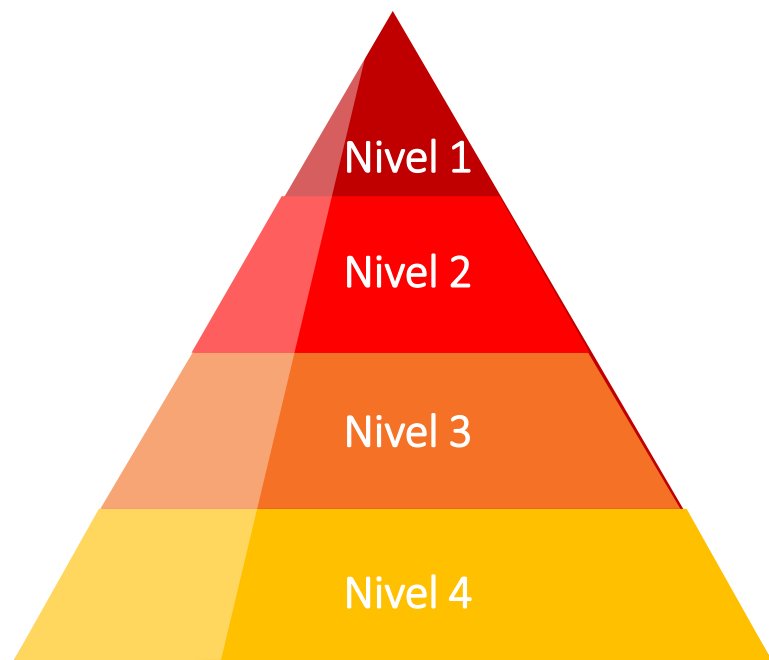
Universidad Complutense de Madrid





MARCO NORMATIVO

Está conformado por todas las normativas y procedimientos de seguridad para dar soporte al cumplimiento del Esquema Nacional de Seguridad y al Reglamento General de Protección de Datos y, por consiguiente, a la protección de los sistemas de información.



- **NIVEL 1 - Política de seguridad de la información**
Establece las directrices para proteger a los sistemas de información.
- **NIVEL 2 - Normativas de seguridad**
Son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Estas políticas deben definir cuáles son los aspectos de la empresa más importantes que deben estar bajo control.
- **NIVEL 3 - Procedimientos de seguridad**
Son la descripción detallada de la manera como se implanta una normativa. El procedimiento incluye todas las actividades requeridas, los roles y responsabilidades de las personas encargadas de llevarlos a cabo.
- **NIVEL 4 - Guías técnicas y manuales de Seguridad**
Las guías técnicas suelen estar dirigidas a profesionales de seguridad, administradores de sistemas y personal técnico, y se centran en aspectos técnicos específicos relacionados con la seguridad. Los manuales de seguridad, por otro lado, están destinados a un público más amplio y pueden abordar tanto aspectos técnicos como no técnicos de la seguridad de la información.



MARCO NORMATIVO

Política de Seguridad



- Documento de alto nivel que define lo que significa 'seguridad de la información'.
- Establece la organización para el gobierno de la seguridad: roles principales
- Debe estar accesible por todos los miembros de la organización
- Debe estar redactado de forma sencilla, precisa y comprensible
- Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos

- **La aprueba la Dirección/Gerencia del organismo**



MARCO NORMATIVO

NORMATIVAS DE SEGURIDAD DE LA INFORMACIÓN

Personal FGUCM

- N. Uso de Recursos y Accesos a Sistemas de Información
- N. Uso y Protección de Portátiles
- N. Gestión de incidentes
- N. Gestión de la clasificación y tratamiento de la Información
- N. Gestión de Activos
- N. Gestión de Soportes
- N. Gestión de autorizaciones
- N. Seguridad Física y del Entorno
- N. Gestión de Acceso Lógico
- N. Gestión de cuentas de usuario
- N. Controles criptográficos
- N. Gestión de redes wifi y bluetooth

Recursos Humanos

- N. Gestión de Formación, Concienciación y Sensibilización
- N. Recursos Humanos
- N. Contratación y Relaciones con Terceros

Contratación

- N. Contratación y Relaciones con Terceros

Desarrollo

- N. Gestión de Desarrollo Seguro

Informática

- N. Gestión de activos
- N. Continuidad del servicio
- N. Gestión de Redes y Comunicaciones
- N. Monitorización
- N. Gestión de Bastionados
- N. Gestión de Ciclo de Vida de las Plataformas Tecnológicas
- N. Gestión del Aseguramiento de Servicios
- N. Gestión del Código Dañino
- N. Gestión del Respaldo de la Información
- N. Gestión Logs de Sistemas y Aplicaciones
- N. Métricas Indicadores de Seguridad
- N. Gestión de autorizaciones

Responsable de Seguridad

- N. Métricas Indicadores de Seguridad
- Cuadro de Mandos



MARCO NORMATIVO

PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Personal FGUCM

- Proc. Comunicación, gestión y respuesta ante incidentes
- Proc. Etiquetado y clasificación de activos e información
- Proc. Adecuación de Documentos
- Proc. Acceso a redes y acceso remoto
- Proc. Gestión de Soportes
- Proc. Uso de Memorias Extraíbles
- Proc. Adquisición, aceptación o autorización

Recursos Humanos

- Proc. Emisión y Control de pases de visita
- Proc. Formación y Concienciación en materia de Seguridad
- Proc. Información sobre derechos y obligaciones del Personal

Contratación

- -

Desarrollo

- Proc. Gestión del Software
- Proc. Paso a producción

Informática

- Proc. Alta, Baja y Modificación de Cuentas de Usuario
- Proc. Asignación, Distribución y Almacenamiento de Contraseñas
- Proc. auditoría y registro (logs)
- Proc. Baja de Equipos - Soportes y Destrucción
- Proc. control de acceso físico al CPD
- Proc. Copias de Seguridad
- Proc. Restaurado de la Información
- Proc. Entrada y Salida de Equipamiento
- Proc. Etiquetado de cableado
- Proc. Gestión de Soportes
- Proc. Gestión de cambios y versiones
- Proc. Gestión de vulnerabilidades técnicas
- Proc. Instalación y despliegue de soluciones software
- Proc. Mantenimiento hardware y software



ROLES

Se han establecido diferentes **responsabilidades** para gestionar y asegurar el cumplimiento de la Seguridad de la Información.

- Comité de Seguridad de la Información
- Responsable de Seguridad de la Información
- Responsable de los Sistemas de Información
- Responsables de los servicios e información
- DPD Delegado de protección de datos



Nuevos roles



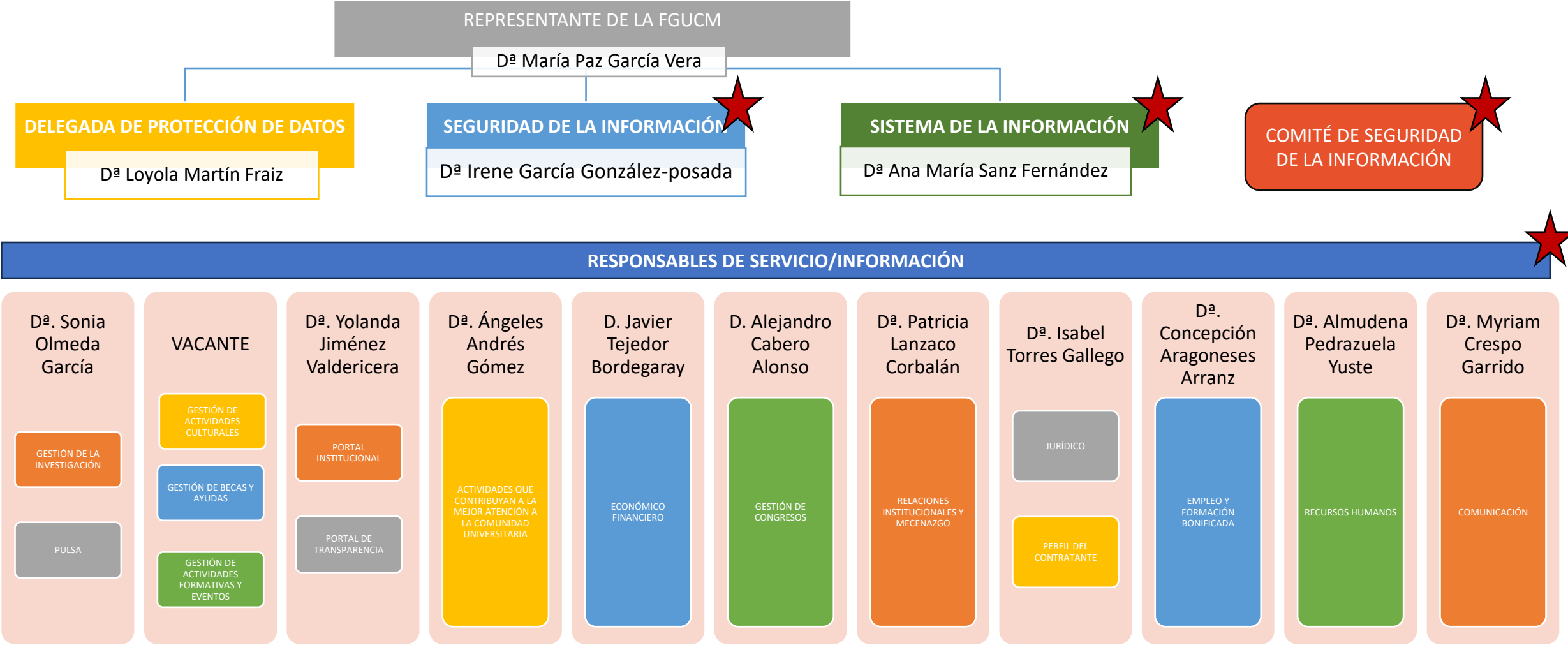
Es muy importante la contribución de **TODOS** a la seguridad de la información



06. Estado actual de la Fundación General de la Universidad Complutense de Madrid

ROLES

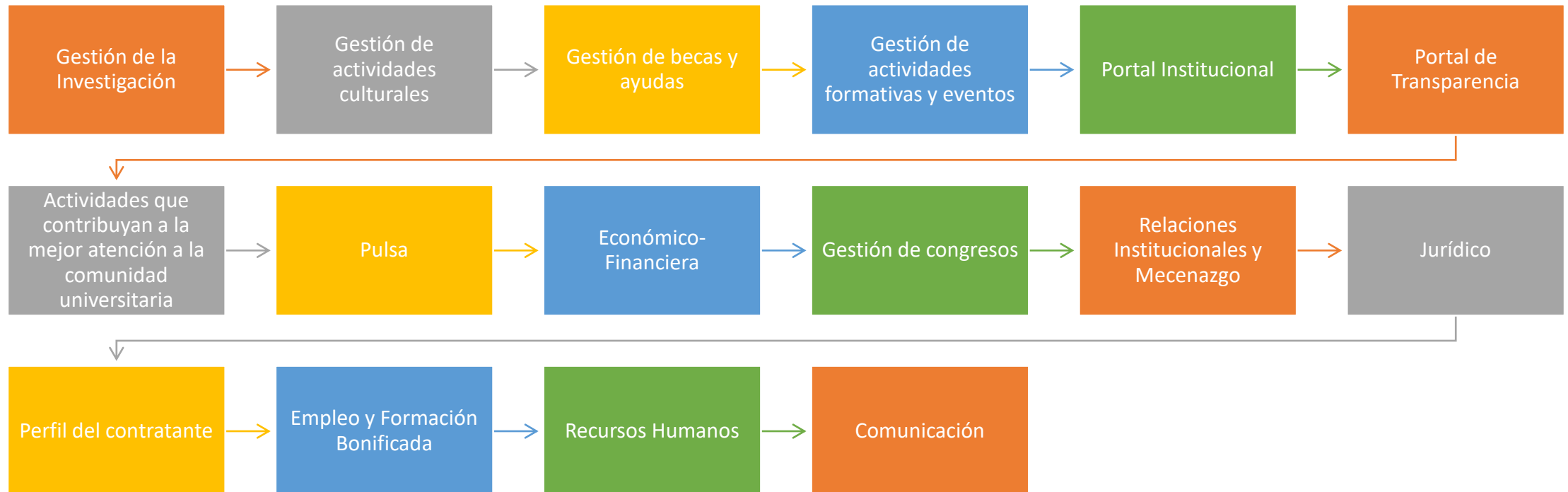
Nuevos roles





Análisis de Riesgos / Plan Director de Seguridad ENS

- Servicios esenciales de la Fundación





Análisis de Riesgos / Plan Director de Seguridad ENS

- Categoría del sistema: MEDIA

Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Medio	Medio	Medio	Medio	Medio

COD	Servicio	CATEGORÍA ENS	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
SENS_01	Gestión de la Investigación	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_02	Gestión de actividades culturales	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_03	Gestión de becas y ayudas	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_04	Gestión de actividades formativas y eventos	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_05	Portal Institucional	MEDIO	Medio	Básico	0	Básico	0
SENS_06	Portal de Transparencia	MEDIO	Medio	Medio	0	Medio	Medio
SENS_07	Actividades que contribuyan a la mejor atención a la comunidad	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_08	Pulsa	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_09	Económico-Financiera	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_10	Gestión de congresos	MEDIO	Medio	Medio	Básica	Medio	Básico
SENS_11	Relaciones Institucionales y Mecenazgo	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_12	Jurídico	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_13	Perfil del contratante	MEDIO	Medio	Medio	Básico	Medio	Medio
SENS_14	Empleo y Formación Bonificada	BÁSICO	Básico	Básico	Básico	Básico	Básico
SENS_15	Recursos Humanos	MEDIO	Medio	Medio	Medio	Medio	Medio
SENS_16	Comunicación	MEDIO	Básico	Medio	0	Medio	Básico



Análisis de Riesgos / Plan Director de Seguridad ENS

- Declaración de aplicabilidad

El ENS exige un mínimo de 73 medidas.

La FGUCM sólo ha de cumplir 68 de ellas porque su sistema se ha categorizado en nivel MEDIO.

	Medidas de Seguridad	Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			Categoría requerida	Autoevaluación de aplicabilidad
			BAJO	MEDIO	ALTO		
			BÁSICA	MEDIA	ALTA		
org	Marco organizativo						
org.1	Política de seguridad	Categoría	aplica	aplica	aplica	BAJO	Si
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica	BAJO	Si
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica	BAJO	Si
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica	BAJO	Si
op	Marco operacional						
op.pl	Planificación						
op.pl.1	Análisis de riesgos	Categoría	aplica	+R1	+R2	MEDIO	Si
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+R1	+R1+R2+R3	MEDIO	Si
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica	BAJO	Si
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+R1	+R1	MEDIO	Si
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica	MEDIO	Si



CUMPLIMIENTO NORMATIVO EL SOA permite a una organización demostrar que ha implementado las medidas de seguridad requeridas por el ENS.



TRANSPARENCIA Y COMUNICACIÓN EL SOA proporciona una visión clara y transparente de las medidas de seguridad implementadas en la organización..



GESTIÓN DE RIESGOS EL SOA ayuda a la organización a identificar y evaluar los riesgos asociados con la seguridad de la información.



GUÍA PARA LA IMPLEMENTACIÓN EL SOA proporciona una guía clara para la implementación de medidas de seguridad.



EVALUACIÓN Y AUDITORÍA EL SOA sirve como referencia para la evaluación y auditoría de la seguridad de la información en la organización



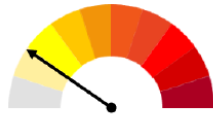
Análisis de Riesgos / Plan Director de Seguridad ENS

Análisis de riesgos

- **IDENTIFICACIÓN:** Identifica los activos que hay que proteger, las amenazas, las vulnerabilidades y su grado de exposición.
- **ANÁLISIS:** Evalúa los riesgos que afectan a la seguridad de la información. Para ello se ha tomado como referencia el ENS.
- **TRATAMIENTO:** Establece medidas para reducir los riesgos a niveles aceptables.



3,9
Riesgo maximo actual
ALTO



1,9
Riesgo maximo actual
BAJO

Escala de Riesgo

(9-10) Catástrofe
(8-9) Desastre
(7-8) Extremadamente crítico
(6-7) Muy crítico
(5-6) Crítico
(4-5) Muy alto
(3-4) Alto
(2-3) Medio
(1-2) Bajo
(0-1) Despreciable



Plan Director de Seguridad

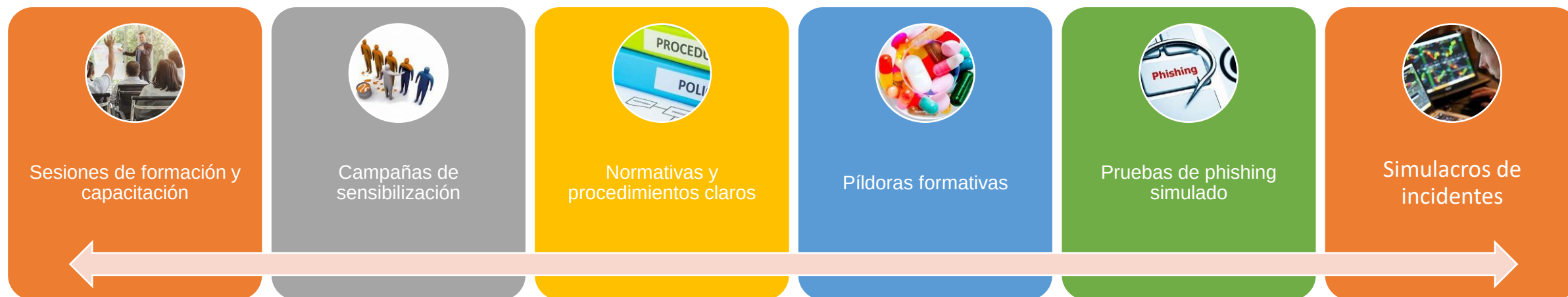
- Es el **conjunto acciones** que se ha diseñado para cumplir con los requisitos mínimos del ENS y para reducir los riesgos identificados en la FGUCM.
- Por cada acción se especifica entre otros datos:
 - Descripción de la acción
 - Prioridad
 - Responsable de ejecutar la acción
 - Dedicación interna
 - Dedicación externa
 - Inversión

HOJA DE RUTA

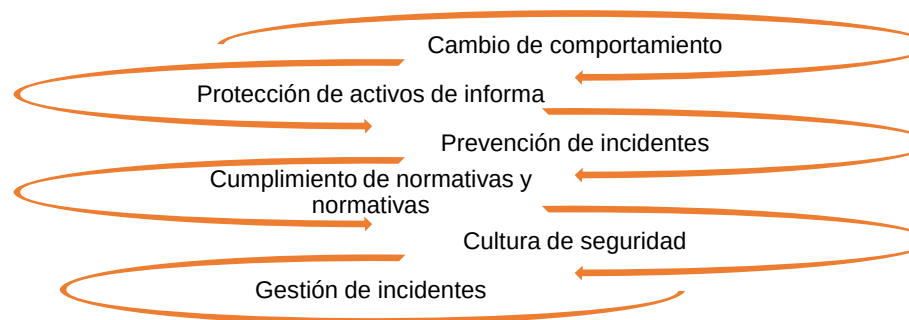
PROYECTOS/SUBPROYECTOS	Prioridad	Acción	Descripción	Responsable Acción	Dedicación Interna	Dedicación externa	Costes 2023	Gastos 2023	Inversión 2023	Costes 2024	Gastos 2024	Inversión 2024
P01 - Política de Seguridad y marco normativo												
01 Acciones Documentales												
DC.001 Fusión del Protocolo de uso de la información	1	Fusión del Protocolo de uso de la información	1.-Fusionar el Protocolo de uso de la información de FGUCM en: -la Normativa de Uso de Recursos y Accesos a Sistemas de Información, para evitar duplicar directrices de seguridad -la Normativa de uso y protección de dispositivos móviles. Asegurar que se incluye "El puesto de trabajo se bloquea al cabo de 10 minutos de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso (equipos de la red administrativa y fuera de esta)". -la Normativa de gestión de soportes. -Tener en cuenta si se debe de incluir alguna indicación en el Procedimiento de Uso de Memorias Extraíbles. -la Normativa sobre los Recursos Humanos, si procede. 2.-Fusionar la guía de buenas prácticas en seguridad de la información en la Normativa de Uso de Recursos y Accesos a Sistemas de Información, para evitar duplicar directrices de seguridad. 3.-Revisar el Protocolo de uso de la información de FGUCM para eliminar referencias de directrices existentes en la normativa de gestión de incidentes o bien, asegurar que no existen contradicciones.	Responsable de Seguridad	24h	0h	6001	-	-	1001	-	-
DC.002 Documento de seguridad	1	Documento de seguridad	Actualizar el Documento de seguridad para: -eliminar directrices duplicadas respecto a las nuevas normativas de seguridad ENS. -insertar referencias de las normativas de seguridad respecto a las nuevas normativas de seguridad ENS -unificar los criterios de clasificación de información e incluir las referencias de las nuevas normativas y procedimientos de seguridad del ENS -traspasar ciertas directrices de seguridad con la normativa de uso de recursos y acceso a los sistemas de información. Se ha de eliminar las directrices del D.S. para no existir directrices duplicadas.	DRD	24h	0h	6001	-	-	1001	-	-
02 Acciones Organizativas												
OR.001 Política de Seguridad	1	Política de Seguridad	Aprobar y difundir la Política de seguridad de la información (la cual debe estar firmada por el Responsable de Seguridad y/o Dirección)	CSJ Responsable de Seguridad	8h	0h	2001	-	-	-	-	-
OR.002 Sección Seguridad en Portal Institucional	2	Sección Seguridad en Portal Institucional	Crear una sección específica de Seguridad de la información en el Portal Institucional, para: -subir toda la documentación relacionada con la Seguridad de la Información. -incluir en el Portal Institucional un enlace directo para acceder a la sección de Seguridad de la Información o bien para subir la Política de seguridad de la información -Incluir directrices relacionadas con el código de ética y la exigencia que se han de instalar en todos los dispositivos	Responsable de Seguridad	16h	0h	4001	-	-	4001	-	-
OR.003 Aceptación de empleados	2	Aceptación de empleados	Recopilar la aceptación de la política de seguridad/política de protección de datos/normativas y procedimientos de seguridad de todos los empleados. Se ha de enviar un correo a cada uno de los empleados informando de dónde está disponible la política de seguridad para que sea leída y que el empleado responda al correo de su aceptación. Estos correos deben de ser custodiados en una carpeta restringida. Siempre se ha de mantener informado a los empleados de las modificaciones de la PSI. Para ello se puede usar muchos métodos, como, por ejemplo, enviar un correo informativo y si es posible un resumen de los cambios producidos	Responsable de Seguridad Dpto. RRHH	16h	0h	5001	-	-	1001	-	-
OR.004 Marco Normativo	1	Marco	1.-Aprobar y difundir las normativas de seguridad.	Responsable de								



Formación / Concienciación



La **concienciación del personal** es una capa esencial de protección, mediante esta se refuerzan las medidas técnicas y organizativas implementadas en la seguridad de la información





Análisis de Impacto (BIA)

- Un análisis de impacto nos permite:



Objetivo: evaluar el impacto financiero, operativo y legal de una interrupción de los servicios y la pérdida de la información.



Proceso: identifica los procesos de negocio críticos, los sistemas de información que los soportan y los activos de datos asociados.



Resultados: permite priorizar las medidas de recuperación y establecer planes de contingencia en caso de desastres.



Evaluación de riesgos: El análisis de impacto permite evaluar y comprender los posibles riesgos y amenazas



Protección de la infraestructura crítica: El análisis de impacto es esencial para proteger la infraestructura crítica de un país, como centrales eléctricas, sistemas de transporte, redes de comunicación y sistemas de suministro de agua..



Planificación de contingencias y respuesta a emergencias: El análisis de impacto proporciona información esencial para la planificación de contingencias y la respuesta a emergencias.



Toma de decisiones basada en evidencia: El análisis de impacto proporciona datos y resultados tangibles que respaldan la toma de decisiones en el ámbito de la seguridad nacional.



Evaluación de la efectividad de las políticas y medidas de seguridad: El análisis de impacto permite evaluar la efectividad de las políticas y medidas de seguridad implementadas en el marco del ENS.



Auditoría Interna ENS

- La auditoría INTERNA es una **revisión** que se lleva a cabo para evaluar si se cumplen con los requisitos del ENS y si los riesgos existentes están controlados.
- Se realizan **entrevistas** con los responsables de las diferentes áreas y por lo tanto se requiere de la colaboración de FGUCM.
- El resultado es un informe dónde se identifican las deficiencias, las cuales hay que solventar.



EVALUACIÓN DE
CUMPLIMIENTO
NORMATIVO



IDENTIFICACIÓN DE
DEBILIDADES Y
BRECHAS



MEJORA DE LA
EFICIENCIA Y
EFICACIA



EVALUACIÓN DE LA
GESTIÓN DE
RIESGOS



FOMENTO DE LA
TRANSPARENCIA Y
LA RENDICIÓN DE
CUENTAS

Es muy importante la COLABORACIÓN de **TODOS**



Auditoría Externa ENS

- La auditoría EXTERNA es una **revisión** que se lleva a cabo para evaluar si se cumplen con los requisitos del ENS y si los riesgos existentes están controlados. **Pero es realizada por una ENTIDAD CERTIFICADORA EXTERNA.**
- Se realizan **entrevistas** con los responsables de las diferentes áreas y por lo tanto se requiere de la colaboración de FGUCM.
- El resultado es un informe dónde se identifican las deficiencias, las cuales hay que documentar, presentar a la entidad certificadora externa y solventar.
- **OBJETIVO FINAL:** obtención de CERTIFICACIÓN DE CONFORMIDAD CON EL ENS (categoría MEDIA), representando que se cumplen con las exigencias mínimas establecidas en el ENS.



Es muy importante la COLABORACIÓN de **TODOS**

Índice

1. ¿Por qué?
2. Esquema Nacional de Seguridad
3. Roles y Responsabilidades
4. Órganos de referencia
5. Estado actual de la Fundación General de la Universidad Complutense de Madrid
6. **Buenas prácticas en seguridad de la información**
7. Dudas y consultas





07. Buenas Prácticas de seguridad de la información

Contraseñas

Directrices

- Cambiarlas frecuentemente
- No las dejes a la vista
- No las compartas con nadie
- No uses la misma para todo

¿Cómo pueden robarnos la contraseña?

- Adivinándola (si es poco robusta)
- Probando (diccionario o fuerza bruta)
- Viéndola (si somos descuidados o la apuntamos)
- Escuchándola (si se la decimos a alguien)
- Pidiéndonosla (Ingeniería social o phishing)
- Sacándola de nuestros dispositivos mediante malware (virus)
- Utilizando herramientas automáticas

- Las claves de acceso se cambian cada 6 meses, obligatoriamente.
- El sistema obliga a usar contraseñas fuertes: (mayúsculas, minúsculas, números y caracteres especiales).

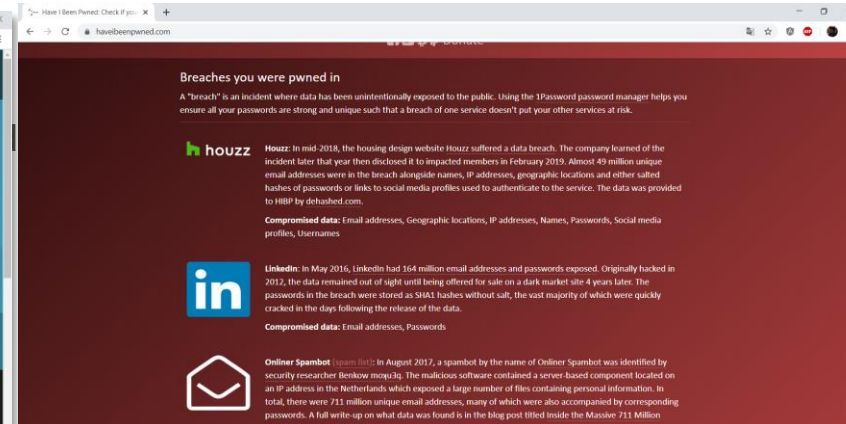
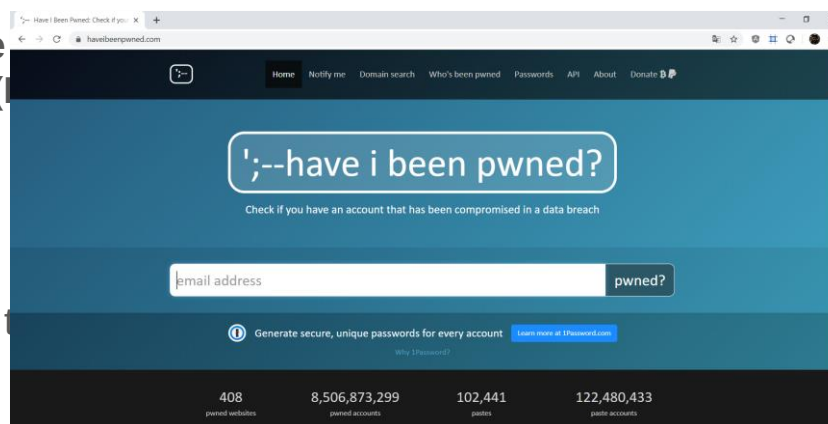


Fundación General
Universidad Complutense de Madrid



- Doble factor de Autenticación (DFA)

- Para conocer si



legger la



07. Buenas Prácticas de seguridad de la información

Contraseñas

Las contraseñas más usadas en España



<https://derechodelared.com/contrasenas-mas-usadas-en-espana/>

Vulnerabilidades de las contraseñas

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

<https://www.infordisa.com/soc/contrasenas-top-10-mas-usadas-2023/>

Prueba tu Contraseña

Contraseña:

Ocultar: ☒

Resultado:

0%

Complejidad: Demasiado corta

Requerimientos recomendados

- Tamaño mínimo de 8 caracteres
- Contener al menos 3-4 de las siguientes cosas:
 - Letras en Mayúsculas
 - Letras en Minúsculas
 - Números
 - Símbolos

<https://www.internautas.org/compruebapassword.html>



07. Buenas Prácticas de seguridad de la información



¿Dónde almacenar las contraseñas?

- Almacenes de contraseñas



- Software gratuito que está a disposición para todos los usuarios de la organización.
- Cuando lo necesites, habla con **Informática** para que te indique qué software de almacenamiento de contraseñas has de usar.



07. Buenas Prácticas de seguridad de la información



- Limpieza y buen uso del papel



- Deja siempre la mesa limpia.
- Guarda los documentos en lugares seguros.
- Evita imprimir documentos innecesarios.
- Recoge los documentos de la impresora.
- Destruye la información usando destructoras de papel.



07. Buenas Prácticas de seguridad de la información



- Wifi “gratuita”
- **Usa sólo redes confiables** (oficina, casa)
- **Nunca** usar redes de conexión gratuita (hoteles, aeropuertos, estación de tren, restaurantes...)



Si el producto es gratis, **TÚ ERES EL PRODUCTO**

Tiene más valor la información que se pierde que el valor del móvil

- ¿Qué pasaría si te robasen el móvil?

Obligaciones

- **Bloqueo**
 - Automático
 - Pin/patrón contraseña, huella, rostro o similar
- **Información**
 - **Limitar la información** sensible contenida
 - **Borre** toda información innecesaria
- **MDM**
 - Solicitar la instalación a Informática cuando cambiemos de móvil.
 - Permite el borrado remoto de la información almacenada en el móvil.
- **Aplicaciones**
 - Descargar apps sólo de repositorios de la organización y/o **tiendas oficiales**
 - **No instales** aplicaciones no corporativas

- **Conexiones**
 - **Desactive** wifi/bluetooth siempre que no sea necesario
 - Evite conectarte a **redes públicas**
 - Evite acceder a **webs no fiables**
- **Configuraciones**
 - Configurar, si es posible, la capacidad de **borrado remoto**
 - **No elimine** las limitaciones de fábrica (rooteo o jailbreak)
 - **Segregue** el uso personal del profesional





¿Cómo cuidar el equipo?

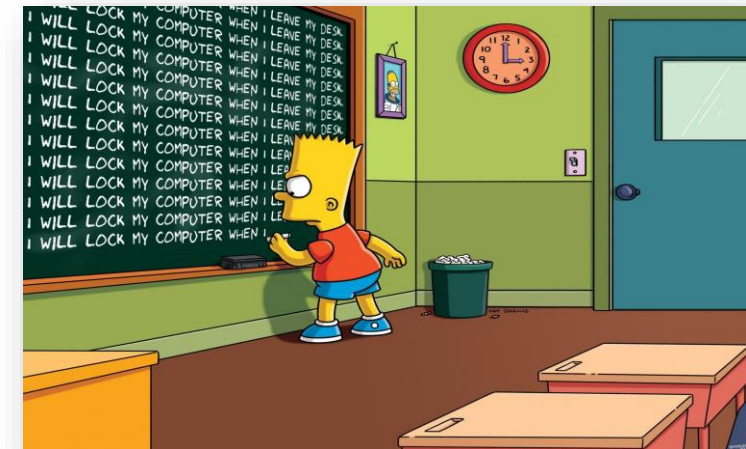
- Apaga el equipo al final del día para que se actualicen las nuevas políticas de seguridad.
- Guarda la información en **INTRANET** o en **SharePoint** y utiliza el mismo mecanismo para **compartirla con terceros**.
- **Bloquea tu ordenador.**

BLOQUEAR SIEMPRE EL EQUIPO cuando abandones tu puesto de trabajo

Aunque sea para:

- Acudir a una reunión.
- Hablar con un compañero.
- Tomarte un descanso corto.

Asegurando que es necesario volver a introducir la contraseña de acceso para poder acceder nuevamente.



No almacenar la información en local

¿Qué es ingeniería social?

- Ingeniería Social

Es un ataque o intento de **obtener información** de las personas mediante **engaño** para:

- Obtener información.
- Instalar un malware con la descarga de archivo.



- **Tipos:**

- Phishing – Vishing – Smishing
- Baiting – Tailgating – Fake News
- Contactos en redes sociales
- Adjuntos “atractivos” en un correo (premios, fotos,...)
- Etc

- **¿Qué buscan?**

- Credenciales de acceso
- Datos de tarjetas de pago
- Instalación de troyanos para atacar un equipo o toda una red
- Información confidencial
- Dinero por pago de rescates

- **¿Qué pueden hacer con la información?**

- Extraer información
- Vender la información
- Fraude
- Intrusión de una red
- Ingresos de dinero
- Suplantar identidad para obtener datos confidenciales



Campaña Phishing

Remitente: rrhh@rrhhfgucm.com

Asunto: Confirmación de datos personales para el nuevo sistema de RRHH

¡ATENCIÓN! Este correo es de remitente externo. Contacte con INFORMATICA@UCM.ES para comprobar mensajes sospechosos.

Buenos días,

Con motivo del traslado a la nueva oficina, nos gustaría saber cuál es tu opinión sobre su ubicación y la zona en cuanto a restauración y ocio. Son solo 4 preguntas, no queremos aburrirte. Eso sí, siendo tan pocas preguntas y viendo lo cerca que está la fecha del traslado, necesitamos que respondas hoy, por favor.

Acceder a la [encuesta](https://rrhhfgucm.com/?id=61946ba9c218286c8d47ad07b868ffac). <https://rrhhfgucm.com/?id=61946ba9c218286c8d47ad07b868ffac>

Gracias a la encuesta.

Gracias a todos.

Atentamente

Laura González Herrera
Responsable de RRHH
+34 91394 6470

PRECAUCIONES

1. Remitente

PRESTAR ATENCIÓN si el correo remitente es conocido y está escrito correctamente.

2. Banner rojo y amarillo

IDENTIFICA CORREO EXTERNO y por lo tanto es FALSO si está relacionado con temas internos.

3. Enlace

PASAR EL RATÓN POR ENCIMA del enlace para comprobar que es una dirección conocida.

4. Firma

COMPROBAR LA FIRMA por si detectas alguna anomalía:

- Nombre del departamento
- Correo electrónico del departamento
- Etc.

MEDIDAS A ADOPTAR

- Si contiene banner rojo/amarillo y solicita información interna es un **CORREO FALSO**

- **NO CONTESTAR**
- **Contactar con INFORMÁTICA**

- Si la URL es desconocida o sospechosa

- **NO CONTESTAR**
- **Contactar con INFORMÁTICA**

- Si no es una tarea habitual

- **NO CONTESTAR**
- **Contacta con el remitente por otra vía**
- **Contactar con INFORMÁTICA**



07. Buenas Prácticas de seguridad de la información



Fundación General
Universidad Complutense de Madrid

Campaña Phishing

Responder Responder a todos Reenviar

ju. 11/04/2019 19:34

Recursos humanos <rrhh@fgucm.es>
Cuadrante de vacaciones de verano

Para ☐ Manuel Gómez García

Documento adjunto (malware).zip
6 KB

Hola,

En el siguiente adjunto podéis encontrar el cuadrante de vacaciones de navidad.

Ruego accedáis y validéis que se os han asignado los días correctos

Responder Responder a todos Reenviar

ju. 11/04/2019 19:34

Recursos Humanos <rrhh.fgucm@gmail.com>
Correo corporativo

Para ☐ Manuela Gómez García

Buenos días,

Se han realizado cambios significativos para actualizar los datos de usuario

Para acceder pulse aquí: [http://mail.nombremoreza\(parecido\).es/owa/auth](http://mail.nombremoreza(parecido).es/owa/auth)

Si tiene alguna pregunta responda directamente

Dirección de Recursos Humanos
rrhh@fgucm.com

Update your Flash Player for Win 10

Windows 10

Adobe Flash Player Update
Install Adobe Flash Player and enjoy the largest database for:

- Music Albums with user-friendly interface
- All Song Formats with easy access
- Videos Library leading video codec library

Decline & Continue Agree & Install

Responder Responder a todos Reenviar

ju. 11/04/2019 19:34

Recursos humanos <rrhh@fgucm.com>
Cuadrante de vacaciones de verano

Para ☐ Manuela Gómez Herrera

Documento adjunto (malware).zip
6 KB

Hola,

En el siguiente adjunto podéis encontrar el cuadrante de vacaciones de navidad. Ruego accedáis y validéis que se os han asignado los días correctos

Dirección de Recursos Humanos
Área de Organización y Recursos Humanos
rrhh@fgucm.com

Libro1.xls...

Archivo Inicio Insertar Diseño de Formas Datos Referencias Vista Desarrollo Indicador Manuel...

Cuidado—los datos adjuntos de correo electrónico pueden contener virus. Si no tiene que realizar ninguna edición, es mejor que siga en Vista protegida.

VISTA PROTEGIDA

Habilitar edición

	A	B	C	D	E
1					
2					



El fraude del CEO

- Ataque que involucra al CEO y/o al Comité de Dirección de una organización y a personas habilitadas a realizar una operación que implique dinero (transferencias, pagos, compras,...)
- Ejemplo:

CEO/Comité de Dirección “ordena” que se realice una transferencia urgente relacionada con una actividad importante que está en curso. Nadie lo discute: Se realiza la transferencia.



Fuente: CCN

¿Cómo prevenirlo?

- Medidas de seguridad técnicas, ya están implementadas por Informática.
- Ante la duda, confirmar la operación con una llamada al CEO auténtico.



07. Buenas Prácticas de seguridad de la información

• Otros tipos de ataques

¿Qué es un Ransomware?

- Malware extremadamente peligroso.
- Aunque no siempre, normalmente se requiere caer en un engaño (correo con adjunto o URL)

¿Cómo se limita?

- No proporcionar los datos de usuario y contraseñas.
- No descargas ficheros sospechosos.
- No hacer clic en enlaces sospechosos.
- Mantener todos los datos en **INTRANET** para que se puedan realizar las copias de seguridad.

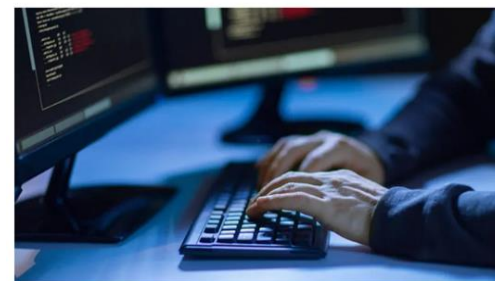


Fundación General
Universidad Complutense de Madrid

07/09/2020

FUNDACIÓN ARIAS CIBERATACADA POR ORTEGUISTAS

“Ataque a sus redes sociales, así como intentos de sabotaje en sus sistemas cibernéticos son algunas de las agresiones virtuales que ha sufrido la Fundación Arias para la Paz y el Desarrollo Humano por parte de grupos afines a Daniel Ortega, presidente de Nicaragua.”.



<https://www.larepublica.net/noticia/fundacion-arias-ciberatacada-por-orteguistas>

11/09/2021

EL CIBERATAQUE A LA UAB AFECTARÁ HASTA FINALES DE AÑO LA DIFÍCIL GESTIÓN DE UNA UNIVERSIDAD SIN ACCESO A SU SISTEMA INFORMÁTICO DURANTE MESES.

El ataque afectó al sistema de virtualización que aloja gran parte de los servicios corporativos de la universidad, lo que a la práctica dejó sin funcionar la página web oficial, los correos oficiales, el Campus Virtual y la red de internet. Alumnos, profesores e investigadores se quedaron sin acceso al sistema informático de la universidad, obstaculizando gran parte de sus tareas diarias.



<https://www.xataka.com/seguridad/ciberataque-a-uab-afectara-finales-ano-dificil-gestion-universidad-acceso-a-su-sistema-informatico-durante-meses>

22/02/2022

LA UOC SUFRE UN RANSOMWARE QUE AECTA ASU CAMPUS VIRTUAL

En octubre le tocó a la Universidad Autónoma de Barcelona. Ahora, a la Universidad Oberta de Catalunya (UOC). Los responsables de la institución catalana alertaron ayer de haber sufrido un ataque informático de tipo ransomware que impide el acceso a su campus virtual.



<https://www.xataka.com/seguridad/uoc-sufre-ransomware-que-afecta-a-su-campus-virtual-asi-ultimo-ciberataque-que-golpea-a-universidad-espanola>



- Fuga de información (involuntaria)

¿Qué es la fuga de información?

Es la **pérdida de confidencialidad de la información** de una organización, mediante la obtención de la misma o el conocimiento del contenido de ésta por parte de personas no autorizadas para ello.

¿Cómo prevenirla?



- Cuidado con la información que se comparte por correo electrónico, puesto que si es sensible debe de ir **cifrada** (protegida con contraseña).
- Usar **OneDrive** como medio de compartir información y siempre a personas autorizadas.



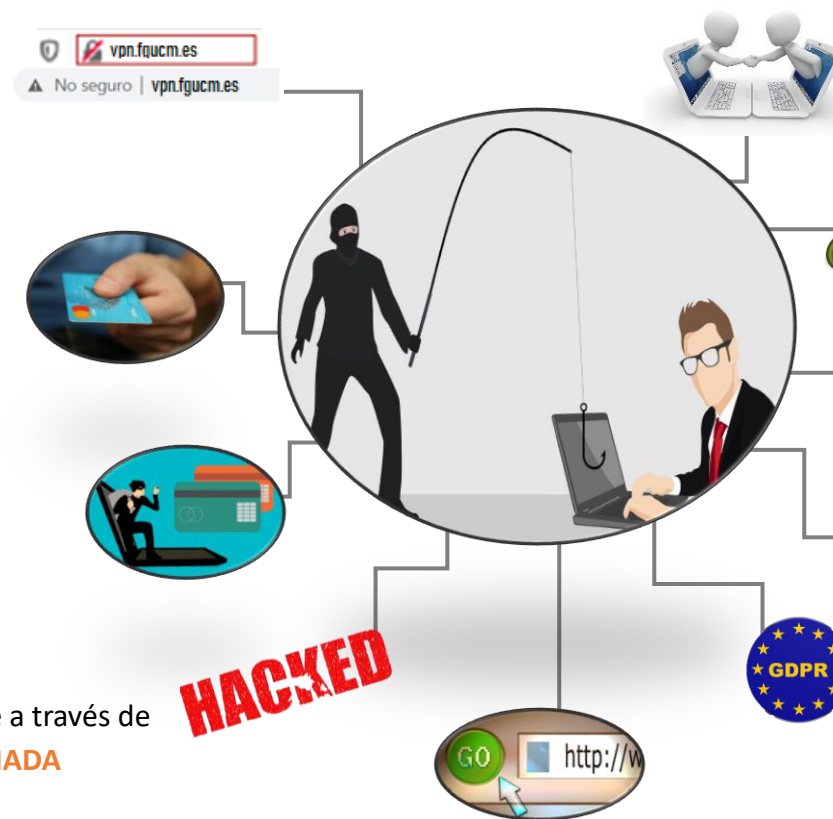
DECÁLOGO BUENAS PRÁCTICAS

10. Sitios webs no seguros. Se identifica por un candado tachado o el mensaje de “No seguro”

9. NO ATENDER a peticiones que **NO** están relacionadas con tu trabajo. O bien, no es una petición habitual.

8. Comprobar ortografía, redacción e idioma del mensaje, puede ser un fraude.

7. Los ataques pueden realizarse a través de CORREO ELECTRÓNICO, LLAMADA TELEFÓNICA o SMS.



1. Presta atención al banner que indica que es un CORREO EXTERNO.

ATENCIÓN! Este correo es de un remitente externo.

2. NO RESPONDER a correos de remitentes desconocidos.

3. NO ABRIR O DESCARGAR ADJUNTOS de los correos, sin verificar antes que el remitente es legítimo.

4. Desconfía de las URL ACORTADAS o que no aparezca la URL. Pasa siempre el ratón sobre la URL para conocer si es una dirección conocida.

5. NO PROPORCIONAR datos sensibles sin autorización (Credenciales, datos personales, datos de organización, etc).

6. NO GUARDAR LAS CONTRASEÑAS EN LOS NAVEGADORES porque se le facilita el acceso a los ciberdelincuentes.

Ante la menor sospecha contacta con el Área de Informática y Nuevas Tecnologías

NO ELIMINAR EL CORREO ELECTRÓNICO



ENVIAR CORREO SOSPECHOSO AL ÁREA DE INFORMÁTICA Y NUEVAS TECNOLOGÍAS



Un comienzo seguro



¡Sentido común!



Y en caso de duda, consulta
con **personal especializado**

¡La seguridad empieza en ti!



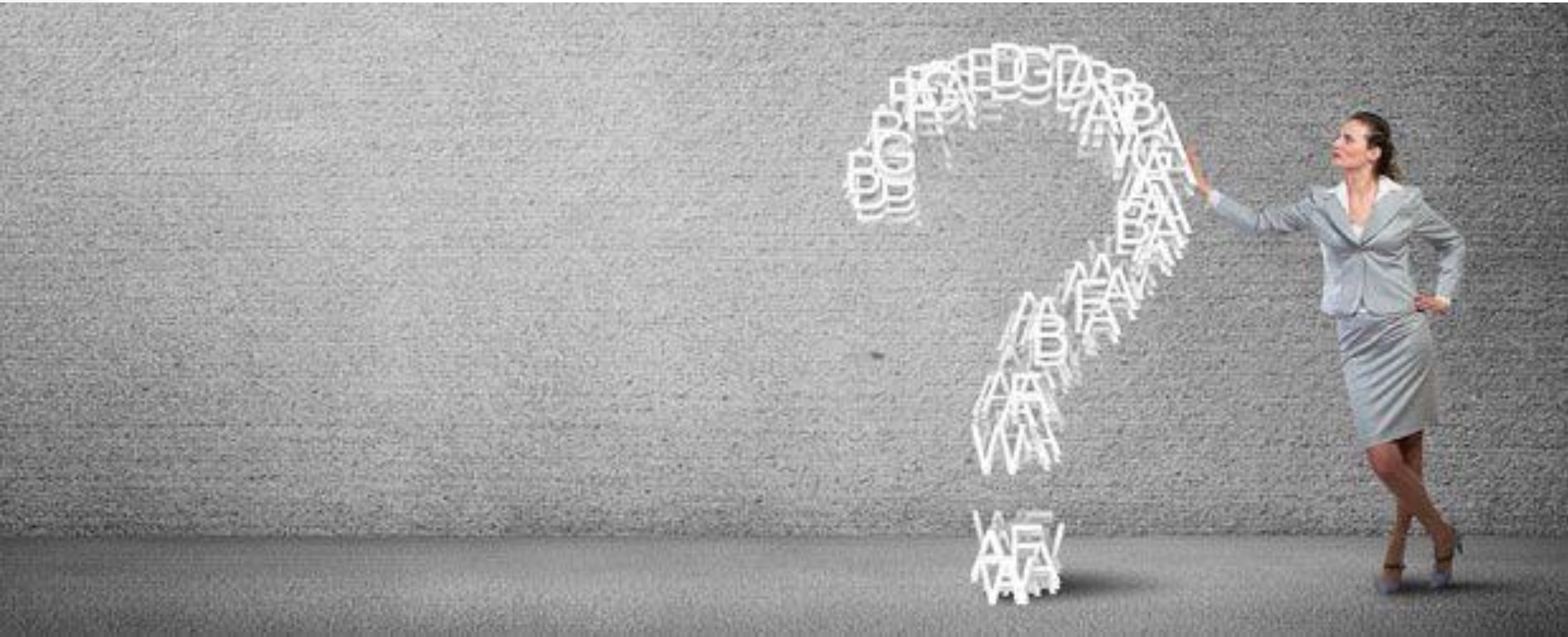
Entre todos
podemos generar
un Clima y una Cultura
de Seguridad
adecuados

Índice

1. ¿Por qué?
2. Esquema Nacional de Seguridad
3. Roles y Responsabilidades
4. Órganos de referencia
5. Estado actual de la Fundación General de la Universidad Complutense de Madrid
6. Buenas prácticas en seguridad de la información
7. **Dudas y consultas**



03. Dudas y consultas





España

Avilés
Barcelona
Madrid
Málaga
Sevilla

Portugal

Lisboa
Proença-a-Nova

Chile

Santiago de Chile

EEUU

New Haven

México

Ciudad de México

Marruecos

Casablanca

www.babelgroup.com

