Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Normativa de Ciberseguridad

UD05. Normativa vigente de ciberseguridad de ámbito nacional e internacional.
Tarea Online 05.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

isftic. *Antena de Telecomunicaciones* (CC BY-NC-SA)

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.

ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.

ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.

Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.

La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.

Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.

En los últimos meses ACME está de enhorabuena, ha logrado la adjudicación de un contrato mayor para la prestación de servicios de comunicaciones a una institución de las Fuerzas y Cuerpos de Seguridad del Estado. Dado el servicio que provee ha sido designado como proveedor de servicio esencial.

Dados los compromisos existentes hasta la fecha y con los nuevos contratos adjudicados, ACME va a abordar el proyecto de despliegue de un Sistema de Gestión de Seguridad de la Información, así como un Sistema de Gestión de Continuidad de Negocio. Asimismo, con el contrato otorgado para Fuerzas y Cuerpos de Seguridad del Estado, debe cumplir con la normativa del Esquema Nacional de Seguridad y con la Directiva NIS.

En esta tarea se requerirá de los conocimientos adquiridos a lo largo de la unidad para desarrollar los contenidos requeridos en el ejercicio.

¿Qué te pedimos que hagas?

Teniendo en cuenta la compañía descrita en el escenario anterior, da respuesta a las siguientes preguntas:

✓ **Apartado 1: Normas nacionales e internacionales**

¿Podrías proponer tres controles de cada proceso de seguridad de la normativa NIST?

Función	Controles
Identificar	1. Desarrollo y actualización de un inventario de activos de información. 2. Definición y aplicación de políticas de gestión de contraseñas robustas. 3. Implementación de controles de acceso físico y lógico a sistemas y datos.
Proteger	1. Implementación de sistemas de detección y prevención de intrusiones. 2. Implementación de sistemas de cifrado para la protección de información confidencial en reposo y tránsito. 3. Establecimiento de controles de seguridad en la gestión de dispositivos móviles y conexión remota a sistemas.
Detectar	1. Establecimiento de sistema de monitorización y registro de actividades en sistemas y redes. 2. Implementación de sistemas de alerta temprana para la detección de incidentes de seguridad. 3. Definición y aplicación de políticas de respuesta a incidentes.
Responder	1. Implementación de sistema de comunicación de incidentes para informar a afectados y autoridades. 2. Desarrollo y mantenimiento de un plan de respuesta a incidentes que contemple la asignación de responsabilidades y la gestión de recursos. 3. Establecer los procesos de análisis post-incidente con los que aprender de errores y mejorar los sistemas de seguridad.
Recuperar	1. Desarrollo y mantenimiento de un plan de recuperación ante desastres que contemple la restauración en el menor tiempo posible, de sistemas y datos. 2. Implementación de sistemas de copia de seguridad y redundancia que garanticen la disponibilidad de datos críticos. 3. Establecimiento de procesos de validación y verificación de sistemas y datos recuperados.

✓ **Apartado 2: Sistema de gestión de seguridad de la información basado en ISO 27001**

- Desarrolla un contexto descriptivo de la organización alineado con los requisitos de información del estándar.
- Propón al menos tres controles para la mitigación de riesgos identificados.
- Desarrolla tres métricas de seguridad para ACME.

ACME S.A. es una empresa española con sede en Madrid que ofrece servicios de telecomunicaciones a particulares y empresas. Cuenta con una amplia cartera de clientes, incluyendo 300.000 en España y presencia en 32 países. **ACME** se caracteriza por su compromiso con la seguridad de la información, lo que le ha permitido obtener la certificación **ISO 27001**.

ACME S.A. ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma **ISO 27001**. Este sistema define los procesos y controles necesarios para proteger la información confidencial, integral y disponible, lo que es fundamental para su éxito en el mercado actual.

	Controles para la mitigación de riesgos
Control de acceso	1. Implementar un sistema de control de acceso basado en roles para restringir el acceso a la información y los recursos de la empresa. 2. Utilizar autenticación MFA para los usuarios con acceso a información confidencial. 3. Implementar un programa de concienciación sobre seguridad para educar a los empleados sobre la importancia de la seguridad de la información.
Protección de datos	1. Encriptar los datos confidenciales en reposo y en tránsito. 2. Implementar un sistema de gestión de parches para asegurar que el software está actualizado. 3. Implementar un sistema de copias de seguridad y recuperación de datos para garantizar la disponibilidad de la información.
Gestión de incidentes	1. Implementar un plan de respuesta a incidentes que defina los roles, responsabilidades y acciones a tomar en caso de un incidente de seguridad. 2. Implementar un sistema de detección de intrusiones para identificar y prevenir ataques a la red. 3. Implementar un programa de análisis forense para investigar los incidentes de seguridad y determinar su impacto.

Métricas de seguridad:

1. **Porcentaje de empleados que han completado la formación en seguridad:** Esta métrica mide el porcentaje de empleados que han recibido formación en seguridad de la información durante el año pasado.
   El objetivo es que el 100% de los empleados reciban formación en seguridad anualmente.
2. **Número de incidentes de seguridad:** Esta métrica mide el número de incidentes de seguridad que han sido reportados durante el año pasado.
   El objetivo es reducir el número de incidentes de seguridad cada año.
3. **Tiempo de respuesta a incidentes:** Esta métrica mide el tiempo que tarda el equipo de seguridad en responder a un incidente de seguridad.
   El objetivo es responder a los incidentes de seguridad en menos de 24 horas.

✓ **Apartado 3: Sistema de gestión de continuidad de negocio basado en ISO 22301**

El escenario a utilizar para este análisis de impacto es del de los sistemas centralizados que dan servicio a la red de comunicaciones de manera centralizada. En caso de indisponibilidad de estos sistemas, la red completa no podría funcionar.

Lucro cesante, provocado por la incapacidad de facturación ocasionada por la parada de los servicios de red. Se estima que la organización factura 100.000 € por hora.

Compensaciones, provocado por los perjuicios que pudieran ocasionar a las empresas a las que ACME da servicio. Según los contratos firmados con los clientes empresa, se garantiza un 99% de servicio, y únicamente se debe compensar en caso de que la caída dure más de 30 minutos, y si el cliente corporativo lo reclama. Se ha estimado que, a partir de la primera hora, las compensaciones supondrían 500.000€ por cada hora de caída.

Imagen, la confianza en la organización y en los servicios que provee se vería afectada. Esto supondría una pérdida de un 1% de la cartera de clientes por cada incidencia. Además, se estima que habría una caída de altas nuevas. Este tipo de perjuicios se ha cuantificado en 200.000€ por incidencia.

Sanciones, la comisión del mercado de las telecomunicaciones puede actuar en caso de una perdida de servicio elevada, además al haber un designio de operador de servicio esencial, una caída prolongada podría ocasionar pérdidas económicas por sanciones.

Se estima que esta situación se daría únicamente en caso de caídas repetidas y de larga duración.

La organización no está dispuesta a asumir perdidas mayores a 1,5 millones de €.

- Realiza un análisis de impacto en continuidad sobre los sistemas asociados al servicio de telecomunicaciones.
- Establece un valor justificado para los parámetros MTPD, RPO y RTO.

Escenario:

Indisponibilidad total de los sistemas centralizados que dan servicio a la red de comunicaciones.

Impactos:

- ✓ **Lucro cesante:** Pérdida de ingresos por facturación: 100.000 €/hora provocado por la parada de servicios que no podrán facturarse durante este periodo.
- ✓ **Compensaciones a clientes:** Pueden ocasionarse grandes perjuicios a los clientes que pueden reclamar por contrato una compensación. En este supuesto es a partir de 30 minutos de caída: 500.000 €/hora.
- ✓ **Daño a la imagen:** la pérdida de confianza en ACME supone también un coste del 1% de la cartera de clientes por incidencia: 200.000 €/incidencia. También supone una caída de altas nuevas.
- ✓ **Sanciones:** Posibles multas por parte de la Comisión del Mercado de las Telecomunicaciones. El ser designado como operador de un servicio esencial, puede provocar pérdidas económicas severas en este aspecto.
- ✓ **Tolerancia al Riesgo:** la organización no está dispuesta a asumir pérdidas mayores a 1,5 millones de €.

Parámetros de Continuidad:

- ✓ **MTPD (Máximo Tiempo de Parada Permitido):** El parámetro representa el tiempo máximo que ACME puede permitirse estar sin servicio antes de que el coste sea inaceptable. Sabemos que han puesto una tolerancia de 1.5 millones, pero

debemos asumir que pueden derivase en base a los impactos analizados costes de diversos tipos. Por ello, otorgamos 1 hora. Se basa en el límite de tiempo para evitar o minimizar las compensaciones a clientes y minimizar también el daño a la imagen.

- ✓ **RPO (Objetivo de Punto de Recuperación):** 30 minutos. Se busca que se acerque al cero para minimizar la pérdida de datos y asegurar la recuperación rápida del servicio.
- ✓ **RTO (Objetivo de Tiempo de Recuperación):** 2 horas. Se busca en este caso un equilibrio entre la complejidad de la recuperación de los servicios y el impacto en el negocio.

✓ **Apartado 4: Esquema nacional de seguridad**

Categoriza los sistemas asociados al servicio de telecomunicaciones en función al escenario definido en el caso práctico, por la prestación de servicios a FCSEs.

Desarrolla una declaración de aplicabilidad justificada.

El proyecto encargado incluye el despliegue de un Sistema de Gestión de Seguridad de la Información, así como un Sistema de Gestión de Continuidad de Negocio.

Como hemos visto en el temario, la categorización de seguridad se establece en función del impacto del incidente en términos de disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad. Si estas dimensiones se ven afectadas, podrán categorizarse en un determinado nivel de seguridad.

Atendiendo al Anexo I del Real Decreto 311/202, y la información facilitada a través del documento BP-14 del CCN-CERT, el siguiente cuadro muestra ambos sistemas, además de algunos de los sistemas que entiendo que son necesarios y van asociados al correcto servicio:

Sistema	Categoría/Nivel	Observaciones
Sistema de Gestión de Seguridad de la Información	Alta	Es fundamental para proteger la información confidencial de la empresa, incluyendo datos de las FCSE. Su indisponibilidad o fallo podría comprometer la seguridad de la información y el cumplimiento de los requisitos legales.
Sistema de Gestión de Continuidad de Negocio	Alta	Un sistema esencial para garantizar la continuidad de las operaciones de la empresa en caso de un incidente. Su indisponibilidad o fallo podría afectar la capacidad de la empresa para prestar servicios a las FCSE, con un impacto significativo en la seguridad pública.
Sistema de acceso a la red	Alta	Estos sistemas permiten a las FCSE acceder a la red de telecomunicaciones y a los servicios que se ofrecen a través de ella. Su indisponibilidad o fallo podría impedir que las FCSE lleven a cabo sus funciones de manera efectiva.

Sistema de almacenamiento de datos	Alta	Almacena datos confidenciales de las FCSE. Su indisponibilidad o fallo podría comprometer la seguridad nacional.
Sistema de seguridad de red	Alta	Estos sistemas son esenciales para proteger la red de telecomunicaciones de ataques cibernéticos y otras amenazas. Su indisponibilidad o fallo podría dejar la red vulnerable a ataques.

1. Declaración de Aplicabilidad

A continuación, se muestra la Declaración de Aplicabilidad del sistema (podrá verse ampliado en el Anexo I):

Código	Descripción	Dimensiones	Nivel de Madurez	Grado Implem.	Cat. Sistema	Valores ajustados
org	**Marco organizativo**					
org.1	Política de seguridad	DICAT	L4	G2	ALTA	aplica
org.2	Normativa de seguridad	DICAT	L4	G2	ALTA	aplica
org.3	Procedimientos de seguridad	DICAT	L4	G2	ALTA	aplica
org.4	Proceso de autorización	DICAT	L4	G2	ALTA	aplica
op	**Marco operacional**					
op.pl	*Planificación*					
op.pl.1	Análisis de riesgos	DICAT	L4	G1	ALTA	+R2
op.pl.2	Arquitectura de Seguridad	DICAT	L4	G1	ALTA	+R1 +R2 +R3
op.pl.3	Adquisición de nuevos componentes	DICAT	L4	G1	ALTA	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D____	L4	G1	MEDIA	+R1
op.pl.5	Componentes certificados	DICAT	L4	G1	ALTA	aplica
op.acc	*Control de acceso*					
op.acc.1	Identificación	___AT	L4	G1	ALTA	+R1
op.acc.2	Requisitos de acceso	_ICAT	L4	G1	ALTA	+R1
op.acc.3	Segregación de funciones y tareas	_ICAT	L4	G1	ALTA	+R1
op.acc.4	Proceso de gestión de derechos de acceso	_ICAT	L4	G2	ALTA	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	_ICAT	L4	G2	ALTA	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	_ICAT	L4	G2	ALTA	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	*Explotación*					
op.exp.1	Inventario de activos	DICAT	L3	G1	ALTA	aplica
op.exp.2	Configuración de seguridad	DICAT	L4	G2	ALTA	aplica
op.exp.3	Gestión de la configuración de seguridad	DICAT	L4	G2	ALTA	+R1 +R2 +R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	DICAT	L4	G2	ALTA	+R1 +R2
op.exp.5	Gestión de cambios	DICAT	L4	G2	ALTA	+R1
op.exp.6	Protección frente a código dañino	DICAT	L4	G2	ALTA	+R1 +R2 +R3 +R4
op.exp.7	Gestión de incidentes	DICAT	L4	G2	ALTA	+R1 +R2 +R3
op.exp.8	Registro de la actividad	____T	L4	G2	ALTA	+R1 +R2 +R3 +R4 +R5
op.exp.9	Registro de la gestión de incidentes	DICAT	L4	G2	ALTA	aplica
op.exp.10	Protección de claves criptográficas	DICAT	L4	G2	ALTA	+R1
op.ext	*Recursos externos*					
op.ext.1	Contratación y acuerdos de nivel de servicio	DICAT	L1	G1	ALTA	aplica
op.ext.2	Gestión diaria	DICAT	L4	G1	ALTA	aplica
op.ext.3	Protección de la cadena de suministro	DICAT	L4	G1	ALTA	aplica
op.ext.4	Interconexión de sistemas	DICAT	L4	G1	ALTA	+R1
op.nub	*Servicios en la nube*					
op.nub.1	Protección de servicios en la nube	DICAT	L1	G1	ALTA	+R1 +R2
op.cont	*Continuidad del servicio*					
op.cont.1	Análisis de impacto	D____	L3	G1	MEDIA	aplica
op.cont.2	Plan de continuidad	D____	L0	G0	n.a.	n.a.
op.cont.3	Pruebas periódicas	D____	L0	G0	n.a.	n.a.
op.cont.4	Medios alternativos	D____	L0	G0	n.a.	n.a.
op.mon	*Monitorización del sistema*					
op.mon.1	Detección de intrusión	DICAT	L4	G2	ALTA	+R1 +R2
op.mon.2	Sistema de métricas	DICAT	L4	G2	ALTA	+R1 +R2
op.mon.3	Vigilancia	DICAT	L4	G2	ALTA	+R1 +R2 +R3 +R4 +R5 +R6
mp	**Medidas de protección**					
mp.if	*Protección de las instalaciones e infraestructuras*					
mp.if.1	Áreas separadas y con control de acceso	DICAT	L4	G1	ALTA	aplica
mp.if.2	Identificación de las personas	DICAT	L4	G1	ALTA	aplica
mp.if.3	Acondicionamiento de los locales	DICAT	L4	G1	ALTA	aplica
mp.if.4	Energía eléctrica	D____	L2	G1	MEDIA	+R1
mp.if.5	Protección frente a incendios	D____	L2	G1	MEDIA	aplica
mp.if.6	Protección frente a inundaciones	D____	L2	G1	MEDIA	aplica
mp.if.7	Registro de entrada y salida de equipamiento	DICAT	L2	G1	ALTA	aplica

mp.per	*Gestión del personal*					
mp.per.1	Caracterización del puesto de trabajo	D I C A T	L0	G0	ALTA	aplica
mp.per.2	Deberes y obligaciones	D I C A T	L0	G0	ALTA	+R1
mp.per.3	Concienciación	D I C A T	L0	G0	ALTA	aplica
mp.per.4	Formación	D I C A T	L0	G0	ALTA	aplica
mp.eq	*Protección de los equipos*					
mp.eq.1	Puesto de trabajo despejado	D I C A T	L3	G1	ALTA	+R1
mp.eq.2	Bloqueo de puesto de trabajo	_ _ _ A _	L3	G1	ALTA	+R1
mp.eq.3	Protección de dispositivos portátiles	D I C A T	L3	G1	ALTA	+R1 +R2
mp.eq.4	Otros dispositivos conectados a la red	_ _ C _ _	L2	G1	ALTA	+R1
mp.com	*Protección de las comunicaciones*					
mp.com.1	Perímetro seguro	D I C A T	L4	G1	ALTA	aplica
mp.com.2	Protección de la confidencialidad	_ _ C _ _	L0	G0	ALTA	+R1 +R2 +R3
mp.com.3	Protección de la integridad y de la autenticidad	_ I _ A _	L0	G0	ALTA	+R1 +R2 +R3 +R4
mp.com.4	Separación de flujos de información en la red	D I C A T	L0	G0	ALTA	+[R2 o R3] +R4
mp.si	*Protección de los soportes de información*					
mp.si.1	Marcado de soportes	_ _ C _ _	L0	G0	ALTA	aplica
mp.si.2	Criptografía	_ I C _ _	L0	G0	ALTA	+R1 +R2
mp.si.3	Custodia	D I C A T	L0	G0	ALTA	aplica
mp.si.4	Transporte	D I C A T	L0	G0	ALTA	aplica
mp.si.5	Borrado y destrucción	_ _ C _ _	L0	G0	ALTA	+R1
mp.sw	*Protección de las aplicaciones informáticas*					
mp.sw.1	Desarrollo de aplicaciones	D I C A T	L0	G0	ALTA	+R1 +R2 +R3 +R4
mp.sw.2	Aceptación y puesta en servicio	D I C A T	L0	G0	ALTA	+R1
mp.info	*Protección de la información*					
mp.info.1	Datos personales	D I C A T	L4	G2	ALTA	aplica
mp.info.2	Calificación de la información	_ _ C _ _	L0	G0	ALTA	aplica
mp.info.3	Firma electrónica	_ I _ A _	L4	G2	ALTA	+R1 +R2 +R3 +R4
mp.info.4	Sellos de tiempo	_ _ _ _ T	L4	G1	ALTA	aplica
mp.info.5	Limpieza de documentos	_ _ C _ _	L0	G0	ALTA	aplica
mp.info.6	Copias de seguridad	D _ _ _ _	L4	G1	MEDIA	+R1
mp.s	*Protección de los servicios*					
mp.s.1	Protección del correo electrónico	D I C A T	L3	G1	ALTA	aplica
mp.s.2	Protección de servicios y aplicaciones web	D I C A T	L4	G1	ALTA	+R2 +R3
mp.s.3	Protección de la navegación web	D I C A T	L4	G1	ALTA	+R1
mp.s.4	Protección frente a denegación de servicio	D _ _ _ _	L4	G1	MEDIA	aplica

Nota 1: El nivel de madurez y el Grado de Implementación, están conformes a la guía CCN-STIC-808.

Nota 2: La columna Cat. Sistema, refleja la categoría (BÁSICA, MEDIA, ALTA) que corresponda en caso de que en esa medida se vean afectadas las cinco (5) dimensiones de seguridad (Confidencialidad- C, Integridad-I, Autenticidad-A, Trazabilidad-T, Disponibilidad-D); si afecta a cualquier categoría del sistema se reflejará 'TODAS'. En caso, de que no se vean afectadas las cinco (5) dimensiones, se reflejará el nivel a aplicar (Bajo, Medio, Alto).

Nota 3: No debe olvidarse que esta Guía refleja un perfil de cumplimiento específico para los sistemas de gestión de seguridad y de continuidad de negocio involucrados en el ámbito de las FCSE, que contempla asimismo ciertos REQUISITOS ESENCIALES o MÍNIMOS de seguridad y protección, siendo lo deseable que las organizaciones que decidan adoptarlo asuman el compromiso de elevar dichas medidas por encima del nivel MEDIO, especialmente en aquellas situaciones en las que un compromiso con la confidencialidad y la integridad se correspondan con los resultados del preceptivo análisis de riesgos.

2. MEDIDAS COMPENSATORIAS

(Detallar aquí las medidas compensatorias, en el momento de haberse aplicado)

3. MEDIDAS COMPLEMENTARIAS DE VIGILANCIA

(Detallar aquí las medidas complementarias de vigilancia, en el momento de haberse aplicado)

4. ACEPTACIÓN DE LA DECLARACIÓN DE APLICABILIDAD

El artículo 28.2 del "RD 311/2022, de 3 de mayo, por el que se regula el ENS", señala "La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad".
En este sentido, como prueba de aceptación, el Responsable de Seguridad suscribe este documento en Madrid, el 23 de marzo de 2024

El Responsable de Seguridad / de Supervisión

ANEXO CUADRO I

Código	Descripción	Dimensiones	Nivel de Madurez	Grado Implem	Cat. Sistem	Valores ajustados
org	**Marco organizativo**					
org.1	Política de seguridad	D I C A T	L4	G2	ALTA	aplica
org.2	Normativa de seguridad	D I C A T	L4	G2	ALTA	aplica
org.3	Procedimientos de seguridad	D I C A T	L4	G2	ALTA	aplica
org.4	Proceso de autorización	D I C A T	L4	G2	ALTA	aplica
op	**Marco operacional**					
op.pl	*Planificación*					
op.pl.1	Análisis de riesgos	D I C A T	L4	G1	ALTA	+R2
op.pl.2	Arquitectura de Seguridad	D I C A T	L4	G1	ALTA	+R1 +R2 +R3
op.pl.3	Adquisición de nuevos componentes	D I C A T	L4	G1	ALTA	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D_ _ _ _	L4	G1	MEDIA	+R1
op.pl.5	Componentes certificados	D I C A T	L4	G1	ALTA	aplica
op.acc	*Control de acceso*					
op.acc.1	Identificación	_ _ _ A T	L4	G1	ALTA	+R1
op.acc.2	Requisitos de acceso	_ I C A T	L4	G1	ALTA	+R1
op.acc.3	Segregación de funciones y tareas	_ I C A T	L4	G1	ALTA	+R1
op.acc.4	Proceso de gestión de derechos de acceso	_ I C A T	L4	G2	ALTA	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	_ I C A T	L4	G2	ALTA	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	_ I C A T	L4	G2	ALTA	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	*Explotación*					
op.exp.1	Inventario de activos	D I C A T	L3	G1	ALTA	aplica
op.exp.2	Configuración de seguridad	D I C A T	L4	G2	ALTA	aplica
op.exp.3	Gestión de la configuración de seguridad	D I C A T	L4	G2	ALTA	+R1 +R2 +R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	D I C A T	L4	G2	ALTA	+R1 +R2
op.exp.5	Gestión de cambios	D I C A T	L4	G2	ALTA	+R1
op.exp.6	Protección frente a código dañino	D I C A T	L4	G2	ALTA	+R1 +R2 +R3 +R4
op.exp.7	Gestión de incidentes	D I C A T	L4	G2	ALTA	+R1 +R2 +R3
op.exp.8	Registro de la actividad	_ _ _ _ T	L4	G2	ALTA	+R1 +R2 +R3 +R4 +R5
op.exp.9	Registro de la gestión de incidentes	D I C A T	L4	G2	ALTA	aplica
op.exp.10	Protección de claves criptográficas	D I C A T	L4	G2	ALTA	+R1
op.ext	*Recursos externos*					
op.ext.1	Contratación y acuerdos de nivel de servicio	D I C A T	L1	G1	ALTA	aplica
op.ext.2	Gestión diaria	D I C A T	L4	G1	ALTA	aplica
op.ext.3	Protección de la cadena de suministro	D I C A T	L4	G1	ALTA	aplica
op.ext.4	Interconexión de sistemas	D I C A T	L4	G1	ALTA	+R1
op.nub	*Servicios en la nube*					
op.nub.1	Protección de servicios en la nube	D I C A T	L1	G1	ALTA	+R1 +R2

op.cont	*Continuidad del servicio*					
op.cont.1	Análisis de impacto	D_ _ _ _	L3	G1	MEDIA	aplica
op.cont.2	Plan de continuidad	D_ _ _ _	L0	G0	n.a.	n.a.
op.cont.3	Pruebas periódicas	D_ _ _ _	L0	G0	n.a.	n.a.
op.cont.4	Medios alternativos	D_ _ _ _	L0	G0	n.a.	n.a.
op.mon	*Monitorización del sistema*					
op.mon.1	Detección de intrusión	DICAT	L4	G2	ALTA	+R1 +R2
op.mon.2	Sistema de métricas	DICAT	L4	G2	ALTA	+R1 +R2
op.mon.3	Vigilancia	DICAT	L4	G2	ALTA	+R1 +R2 +R3 +R4 +R5 +R6
mp	**Medidas de protección**					
mp.if	*Protección de las instalaciones e infraestructuras*					
mp.if.1	Áreas separadas y con control de acceso	DICAT	L4	G1	ALTA	aplica
mp.if.2	Identificación de las personas	DICAT	L4	G1	ALTA	aplica
mp.if.3	Acondicionamiento de los locales	DICAT	L4	G1	ALTA	aplica
mp.if.4	Energía eléctrica	D_ _ _ _	L2	G1	MEDIA	+R1
mp.if.5	Protección frente a incendios	D_ _ _ _	L2	G1	MEDIA	aplica
mp.if.6	Protección frente a inundaciones	D_ _ _ _	L2	G1	MEDIA	aplica
mp.if.7	Registro de entrada y salida de equipamiento	DICAT	L2	G1	ALTA	aplica
mp.per	*Gestión del personal*					
mp.per.1	Caracterización del puesto de trabajo	DICAT	L0	G0	ALTA	aplica
mp.per.2	Deberes y obligaciones	DICAT	L0	G0	ALTA	+R1
mp.per.3	Concienciación	DICAT	L0	G0	ALTA	aplica
mp.per.4	Formación	DICAT	L0	G0	ALTA	aplica
mp.eq	*Protección de los equipos*					
mp.eq.1	Puesto de trabajo despejado	DICAT	L3	G1	ALTA	+R1
mp.eq.2	Bloqueo de puesto de trabajo	_ _ _A_	L3	G1	ALTA	+R1
mp.eq.3	Protección de dispositivos portátiles	DICAT	L3	G1	ALTA	+R1 +R2
mp.eq.4	Otros dispositivos conectados a la red	_ _C_ _	L2	G1	ALTA	+R1
mp.com	*Protección de las comunicaciones*					
mp.com.1	Perímetro seguro	DICAT	L4	G1	ALTA	aplica
mp.com.2	Protección de la confidencialidad	_ _C_ _	L0	G0	ALTA	+R1 +R2 +R3
mp.com.3	Protección de la integridad y de la autenticidad	_I_A_	L0	G0	ALTA	+R1 +R2 +R3 +R4
mp.com.4	Separación de flujos de información en la red	DICAT	L0	G0	ALTA	+[R2 o R3] +R4
mp.si	*Protección de los soportes de información*					
mp.si.1	Marcado de soportes	_ _C_ _	L0	G0	ALTA	aplica
mp.si.2	Criptografía	_IC_ _	L0	G0	ALTA	+R1 +R2
mp.si.3	Custodia	DICAT	L0	G0	ALTA	aplica
mp.si.4	Transporte	DICAT	L0	G0	ALTA	aplica
mp.si.5	Borrado y destrucción	_ _C_ _	L0	G0	ALTA	+R1

mp.sw	*Protección de las aplicaciones informáticas*						
mp.sw.1	Desarrollo de aplicaciones	D I C A T	L0	G0	ALTA	+R1 +R2 +R3 +R4	
mp.sw.2	Aceptación y puesta en servicio	D I C A T	L0	G0	ALTA	+R1	
mp.info	*Protección de la información*						
mp.info.1	Datos personales	D I C A T	L4	G2	ALTA	aplica	
mp.info.2	Calificación de la información	_ _C_ _	L0	G0	ALTA	aplica	
mp.info.3	Firma electrónica	_I_A_	L4	G2	ALTA	+R1 +R2 +R3 +R4	
mp.info.4	Sellos de tiempo	____T	L4	G1	ALTA	aplica	
mp.info.5	Limpieza de documentos	_ _C_ _	L0	G0	ALTA	aplica	
mp.info.6	Copias de seguridad	D____	L4	G1	MEDIA	+R1	
mp.s	*Protección de los servicios*						
mp.s.1	Protección del correo electrónico	D I C A T	L3	G1	ALTA	aplica	
mp.s.2	Protección de servicios y aplicaciones web	D I C A T	L4	G1	ALTA	+R2 +R3	
mp.s.3	Protección de la navegación web	D I C A T	L4	G1	ALTA	+R1	
mp.s.4	Protección frente a denegación de servicio	D____	L4	G1	MEDIA	aplica	

Nota 1: El nivel de madurez y el Grado de Implementación, están conformes a la guía CCN-STIC-808.