GUÍA DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD

Salma Nah Mohamed

Contenido

INTRODUCCIÓN Y OBJETO 2
DEFINICIONES SEGÚN GUÍA 806 3
REFERENCIAS 3
Documentos relacionados 3
DESARROLLO 4
Política de seguridad 4
Categorización de los sistemas 4
Protección de datos de carácter personal 6
Análisis de riesgos 7
Declaración de Aplicabilidad 8
Insuficiencias del sistema 8
ANEXOS 18
Anexo I: Política de Seguridad 18
Anexo II: Declaración de Aplicabilidad (SOA) 22
Anexo III Plan de mejora seguridad 32
Anexo IV Análisis de Riesgos 45
BIBLIOGRAFIA 60

INTRODUCCIÓN Y OBJETO

Tal y como se recoge en el Real Decreto 3/2010, el Esquema Nacional de Seguridad (en adelante, ENS) persigue aumentar "la confianza en que los sistemas de información prestan sus servicios y custodian la información", a través de un conjunto de requerimientos relacionados con la seguridad de la información.

El ámbito de aplicación queda circunscrito, no de forma exhaustiva, a los sistemas de información de la Administración Electrónica, siendo este ampliable a aquellas organizaciones privadas que le proporcionen soluciones tecnológicas o servicios comprendidos dentro del ámbito objetivo de aplicación del Esquema Nacional de Seguridad. Por ejemplo, si el Ayuntamiento X decidiese externalizar el servicio de monitorización de los sistemas del consorcio, debe asegurarse de que las empresas que se presenten para dicho servicio se encuentren certificadas en el ENS.

En este sentido, *Newco*, como proveedor hosting y housing, ha definido como principal objetivo estratégico ser un potencial proveedor y colaborador de la Administración. Newco, consciente de que debe cumplir con el ENS para poder entrar en el proceso de licitación, contrata los servicios de una consultoría tecnológica con el objeto de conseguir una correcta adecuación al ENS.

Newco es una empresa tecnológica dedicada a ofrecer hosting y housing a terceros y, en el caso que nos compete, a la administración pública. Newco dispone de dos servidores físicos propios en un centro de datos, donde albergan máquinas virtuales de los más de sus cien clientes, y un CPD.

Para dar cumplimiento a lo mencionado anteriormente, el presente documento tiene como objeto recopilar en único documento los principios y requisitos mínimos según lo requerido por la Ley 3/2010 por la que se regula el Esquema Nacional de Seguridad (en adelante ENS), correspondientes a la fase de adecuación de la entidad que tienen cabida en *Newco* dentro del marco del ENS.

Este documento ha sido elaborado tomando como referencia la guía STIC-806 del Centro Criptológico Nacional, la cual requiere que se definan los siguientes contenidos:

- Política de seguridad
- Información que se maneja, con su valoración
- Servicios que se prestan, con su valoración
- Datos de carácter personal
- Categoría del sistema
- Análisis de riesgos
- Declaración de aplicabilidad
- Insuficiencias del sistema
- Plan de mejora seguridad

Igualmente, se han tenido en consideración las guías FEMP TOMO, en las se establecen pautas para ayudar a las Administraciones Locales a interpretar de forma práctica y homogénea las obligaciones derivadas del Esquema Nacional de Seguridad.

Asimismo, para abordar de manera correcta la mencionada adecuación se contará con la colaboración, mediante entrevistas, de expertos que han abordado el proceso de adecuación al ENS en sus respectivas organizaciones.

Sin embargo, y hasta la actualidad, no existe una guía específica de implantación del ENS para las empresas privadas, pese a que más del 70% de las certificaciones corresponden al sector privado.

En lo que respecta a la planificación, se irá abordando según se vaya avanzando las tareas requeridas para la adecuación del ENS y dependiendo del estado de madurez de la entidad.

DEFINICIONES SEGÚN GUÍA 806

- **Análisis de riesgos:** Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.
- **Datos de carácter personal:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- **Información:** Caso concreto de un cierto tipo de información.
- **Política de seguridad:** Conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.
- **Responsable de la seguridad:** El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- **Servicio:** Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.
- **Sistema de información:** Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

REFERENCIAS

Documentos relacionados

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE de 23 de junio de 2007.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

DESARROLLO

A continuación, se detallan los diferentes contenidos, estructurados en siete bloques.

Política de seguridad

El Esquema Nacional de Seguridad, en su Artículo 11 y la vez en el punto 3.1 del ANEXO II, establece que la organización debe disponer de una Política de Seguridad que determine los requisitos mínimos de seguridad que han cumplir los sistemas de información.

Newco dispone de una Política de Seguridad que es de aplicación a todos los sistemas de información determinados en el Alcance del SIG, así como a todos los miembros de la entidad y personal externo contratado, sin excepciones.

Así pues, la Dirección de *Newco* constata su firme y explícito compromiso conforme a la Seguridad en sus sistemas y aprueba la Política de Seguridad de la Información, cuyo propósito es establecer las directrices a seguir en materia de seguridad. La Política de Seguridad puede ser consultada en el Anexo I.

Las insuficiencias detectadas, se han analizado y se han propuesto las correcciones adecuadas en el Plan de Mejora del presente documento.

Categorización de los sistemas

Según el Artículo 43 del ENS, se establece la necesidad de determinar la categoría del sistema o sistemas de información, incluyendo los activos esenciales (información y servicios) y valorando el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información. Adicionalmente, dicho impacto podría acarrear repercusiones negativas a la hora de:

- Alcanzar sus objetivos
- Proteger los activos que dan respaldo a la organización
- Cumplir con los acuerdos de nivel de servicio
- Cumplir con la regulación vigente
- Respetar los derechos de los ciudadanos

La categorización se realiza valorando, según las dimensiones de seguridad afectadas (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad), el nivel de impacto en dichas dimensiones (BAJO, MEDIO o ALTO).

Las dimensiones de seguridad son:

- **Disponibilidad**: Consecuencias que tendría que una persona o sistema interconectado autorizado no pudiera usar el servicio cuando lo necesita dentro del periodo de servicio establecido y anunciado por la organización.
- **Confidencialidad**: Consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

- **Integridad**: Consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.
- **Autenticidad**: Consecuencias que tendría el hecho de que la información no fuera auténtica.
- **Trazabilidad**: Consecuencias que tendría el no poder comprobar a posteriori quién ha accedido a, o modificado, una cierta información.

Es importante recalcar que no todas las dimensiones tienen aplicabilidad en servicios e información, siendo estos divididos en:

Dimensión	Servicio	Información
Disponibilidad	Aplica	No aplica
Integridad	No aplica	Aplica
Confidencialidad	No aplica	Aplica
Autenticidad	No aplica (salvo que sea de interés)	Aplica
Trazabilidad	No aplica (salvo que sea de interés)	Aplica

Para la valoración, se han seguido los criterios que propone la guía STIC-803 del Centro Criptológico Nacional de Valoración de los sistemas para servicios e información de los sistemas que entran dentro del alcance del proyecto de adecuación. Los criterios que se han seguido son entre otros:

- Incumplimiento de una Norma
  - Legal
  - Regulatoria
  - Contractual
  - Interna
- Pérdidas económicas
- Reputación
- Protestas
- Delitos
- Datos de carácter personal con carácter general.
  - Cantidad considerable de datos personales
  - Importante riesgo para los derechos y libertades de los interesados
  - Evaluación sistemática y exhaustiva de aspectos personales
  - Control de zonas de acceso público a gran escala
- RTO

El resultado de la valoración, para cada activo esencial es el siguiente:

Activo esencial	Dimensión	Valoración
SOC (Centro de operaciones de seguridad)	D	A
	I	
	C	
	A	
	T	
Arquitectura de configuración de cliente	D	
	I	M
	C	A
	A	M
	T	M
Proyecto Consultoría	D	B
	I	
	C	
	A	
	T	
Información de cliente	D	
	I	M
	C	A
	A	M
	T	M
Monitorización 24x7 (comunicaciones sistemas)	D	A
	I	
	C	
	A	
	T	
Soporte Usuarios 8x5	D	A
	I	
	C	
	A	
	T	
Arquitectura de configuración [24x7 + 8x5]	D	
	I	M
	C	A
	A	M
	T	M

Protección de datos de carácter personal

Los sistemas de información circunscritos en el alcance tratan datos de carácter personal. Se requiere pues, un adecuado cumplimiento de la legislación vigente en materia de protección de datos personales, a saber:

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

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

Se disponen de Registros de Actividades de Tratamiento de los siguientes departamentos:

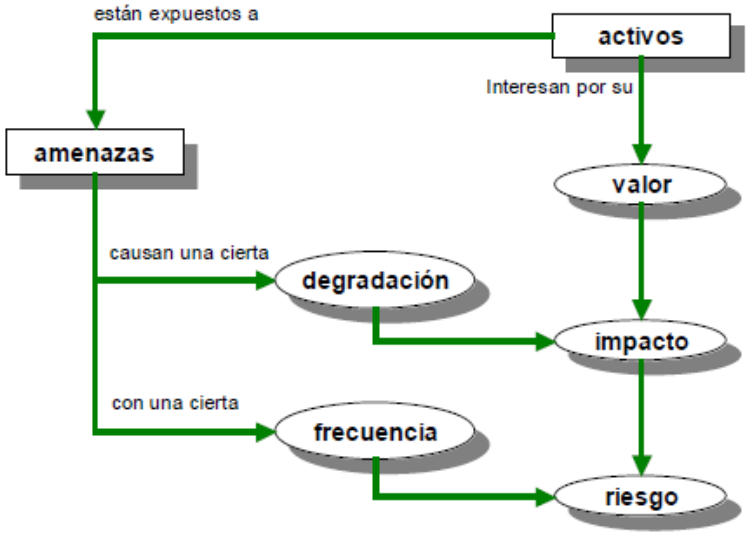
- Finanzas
- Personas
- Sistemas
- Marketing
- Ciberseguridad

Análisis de riesgos

Newco ha realizado un Análisis de Riesgo a través de la herramienta del Centro Criptológico Nacional "PILAR". Esta herramienta, basada en la metodología internacionalmente reconocida MAGERIT v3, ha ayudado durante la fase de apreciación de riesgos a la identificación, evaluación y tratamiento de los riesgos de la entidad. Esta metodología, elaborada por el Consejo Superior de Administración Electrónica, está basada en las siguientes fases:

- Determinación y valoración de activos críticos/relevantes de la entidad
- Establecer amenazas a las que están expuestos los activos
- Determinar las salvaguardas establecidas y cuales son eficaces frente al riesgo.
- Estimación del impacto
- Estimación del riesgo, asociando la tasa de ocurrencia (probabilidad) de la amenaza al impacto.

Un esquema resumen se podría definir de la siguiente manera:



Respecto a los niveles de riesgo aceptables, la Dirección General de Newco ha decidido tomar como valor aceptable, en una escala de 0 a 10 puntos, el valor de **2,6 unidades de riesgo**.

Declaración de Aplicabilidad

La declaración de aplicabilidad implica una relación de medidas en las que se muestran los requisitos del Anexo II del ENS y su aplicabilidad en los diferentes sistemas o subsistemas. Además, asociados a cada medida, se encuentra un conjunto de dimensiones definidos por una dimensión concreta de la seguridad. Se adjunta en el Anexo III la Declaración de Aplicabilidad por su extensión.

Insuficiencias del sistema

Se registran a continuación el resumen de insuficiencias detectadas en los sistemas de NewCo respecto al conjunto de medidas exigidas en el Anexo II del ENS. Este resumen, conocido comúnmente como Declaración de Aplicabilidad, incluye una columna de apoyo que señala el estado actual de cada medida a través de un CMM (Capability Maturity Model) o Modelo de Madurez de Capacidades, según los siguientes criterios:

Modelo Madurez (basado en guía CCN-STIC-804)	
Nivel	Descripción
L0	**Incompleto** Esta medida no está siendo aplicada en este momento.
L1	**Inicial/ad hoc** En el nivel L1 de madurez, el proceso existe, pero no se gestiona. La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad.
L2	**Repetible** En el nivel L2 de madurez, la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo. (Control implantado y establecido formalmente. Se aplica de manera eficaz y siempre se ejecuta del mismo modo).
L3	**Definido** Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3. (Control implantado, establecido formalmente y documentado).
L4	**Gestionado** Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel L3, la confianza era solamente cualitativa. (Control implantado, establecido formalmente, documentado, revisado periódicamente y con métricas asociadas).
L5	**Optimizado** El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores. (Control implantado, establecido formalmente, documentado, con indicadores asociados y sujeto a mejora continua).

Factores atenuantes y agravantes

Los criterios anteriormente indicados están sujetos a la interpretación del equipo consultor. Asimismo, cabe señalar que, en aquellos casos en los que los requisitos se cumplan de forma general, pero se detecten evidencias de incumplimiento parcial, el equipo consultor puede reducir el nivel de cumplimiento asignado. De igual forma, en caso de detectar medidas adicionales extraordinarias, o un alto nivel de cumplimiento del control analizado sin que este requiera ser documentado o medido, el equipo consultor puede aumentar el nivel de madurez sin que implique una traslación exacta de los criterios establecidos.

Se detallan a continuación las insuficiencias detectadas durante la fase de adecuación al ENS:

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
org.1	Política de seguridad	L2	La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización no está reflejado en la política. Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso no está reflejado en la política. Los roles y responsabilidades de la política actuales no están alineados con los identificados en la documentación del SIG del Esquema (Roles y Responsabilidades) No se han formalizado las responsabilidades a las personas físicas correspondientes. No se han formalidad comités correspondientes. Requiere de aprobación por la Dirección (por ejemplo, a través de la firma)
org.2	Normativa de seguridad	L2	La responsabilidad del personal con respecto al cumplimiento o violación de estas normas derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente es un requisito que no se refleja en la normativa.
org.3	Procedimientos de seguridad	L2	Los procedimientos de seguridad en su estado actual, no establecen las fases y acciones por las que pasa cada procedimiento en la casuística real, por lo que no cumple con los requisitos y están obsoletos. Además, gran parte de los procedimientos que debería haber, son inexistentes. No se registra quién es el responsable de las mismas y se ha detectado una carencia de qué tareas debe realizar cada departamento que forma tiene parte en las diferentes acciones de los procesos.
org.4	Proceso de autorización	L2	Algunos procedimientos de seguridad no contemplan la necesidad de solicitud de autorización según necesidades de los empleados o sistemas.
op.pl.1	Análisis de riesgos	L0	No se ha realizado un análisis de riesgos.
op.pl.2	Arquitectura de seguridad	L0	El documento requerido no existe en el sistema de gestión de NewCo, aunque la información que debería ir documentada se deposita en las diferentes áreas de conocimiento y registros. Se requiere incluir: - Mapa de instalaciones en las que se detallen las diferentes zonas (publicas, internas, recepción de material, seguras) - Inventario completo y actualizado - Un esquema de red actualizado que refleje el estado del alcance. -- Un esquema de líneas de defensa

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
			- Los diferentes sistemas de identificación y autenticación de las aplicaciones.
op.pl.2	Arquitectura de seguridad	L0	El documento requerido no existe en el sistema de gestión de Nexco. Requiere incluir el punto e) de la medida
op.pl.2	Arquitectura de seguridad	L0	El documento requerido no existe en el sistema de gestión de Nexco. Requiere incluir el punto f) de la medida
op.pl.3	Adquisición de nuevos componentes	L1	El documento requerido no existe en el sistema de gestión de la entidad. No existe un proceso formal que planifique, desde un punto de vista de la seguridad, la adquisición de los componentes. Los nuevos productos no se tienen en cuenta durante la apreciación de riesgos, previa a su incorporación o no hay documentación que así lo demuestre. No existe un documento de arquitectura de seguridad.
op.pl.4	Dimensionamiento / Gestión de capacidades	L1	No se dispone de procedimientos al respecto que, en caso de implantación de un sistema, éste se dimensione y se planifique en vista del crecimiento que pueda ocasionar en un futuro. Durante el proceso de detección de insuficiencias, no se ha detectado un claro ejemplo de incidentes o problemas de dimensionamiento, los cuales podrían haber surgido por el crecimiento de la entidad en lo que a personal y transformación digital respecta.
op.pl.5	Componentes certificados	L0	Para los sistemas existentes no se dispone de evidencia que demuestre que se realice un proceso de evaluación de las funcionalidades de seguridad y que cuenten con un certificado reconocido por el CCN, Common Criteria o LINCE. De esta forma, no existe un proceso de adquisición de componentes certificados para los productos de seguridad
op.acc.1	Identificación	L2	No se dispone de documento que cumpla con lo requerido, aunque se cumplen algunos de los requisitos en la designación de identidades en los SI. Además, se ha detectado estas reglas no se cumplen de forma correcta y que existe un conjunto de cuentas de administrador que se usan en común por un conjunto de usuarios.
op.acc.2	Requisitos de acceso	L1	En el alcance del ENS existen 46 usuarios administradores del dominio. 1. Existen varios usuarios genéricos pendientes de revisión para deshabilitar. 1. Se debe disponer de arquitectura. 2. Todos los administradores tienen el mismo nivel de permisos sobre configuración y registros. Separar funcionalidades. 3. Se debe disponer de inventario de registros de auditoría. Esta medida no se cumple. 4. Se debe revisar periódicamente el registro de auditoría. Este requerimiento no se cumple.
op.acc.3	Segregación de funciones y tareas	L1	Los usuarios son administradores de los equipos, no segregándose las cuentas en dos partes: usuario y administración Existe una incompatibilidad, tal y como se indica en el requisito b)
op.acc.4	Proceso de gestión de derechos de acceso	L2	Se controla autorización a recursos, por grupos, pero debe revisarse quién es el responsable de autorizar dichos recursos. Respecto al punto a), se ha determinado la posibilidad de que un usuario pueda acceder a contenido de otros departamentos.

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
op.acc.5	Mecanismo de autenticación	L1	Los mecanismos de autenticación son mínimos para el acceso a los sistemas de información. No se dispone de un documento que haga constar los mecanismos de autenticación de los empleados. El acceso a los repositorios de contraseñas más comunes han sido: - Repositorios de contraseñas en sistemas de archivos comunes (debidamente protegidos pero sin trazabilidad), - Hojas de cálculo sin proteger con contraseñas, - Contraseñas por defecto en post-it's. No existe una periodicidad definida respecto a la no utilización de las cuentas. Se detecta que los diferentes sistemas del departamento del seguridad no cumple con la política de contraseñas establecido por las Normas de Seguridad de NewCo.
op.acc.5	Mecanismo de autenticación	L0	No se dispone de sistema de doble autenticación para el acceso a los sistemas de información que entran dentro del alcance. Las aplicaciones que no cumplen con los requisitos mínimos de calidad y renovación de contraseñas deben cumplir con las políticas de contraseñas definidas por la entidad. No se dispone de un proceso que refleje lo anteriormente mencionado.
op.acc.5	Mecanismo de autenticación	L0	No se suspenden las credenciales tras un tiempo de inactividad, ni se refleja en un procedimiento. Por el contrario, las contraseñas generalmente caducan según un tiempo definido.
op.acc.6	Acceso local (local logon)	L0	Se incumplen los requisitos: El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos. El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.
op.acc.6	Acceso local (local logon)	L0	No se está informando al usuario del último acceso correcto
op.acc.6	Acceso local (local logon)	L0	No se han definido restricciones de horario No se han detectado o analizado puntos de renovación de autenticación
op.acc.7	Acceso remoto (remote login)	L3	Los sistemas de información que entran dentro del alcance pueden ser accedidos desde entornos remotos, sin necesidad de conexión cifrada VPN.
op.acc.7	Acceso remoto (remote login)	L3	Se dispone de política de uso, pero no contempla explícitamente lo que se puede hacer de forma remota
op.exp.01	Inventario de activos	L3	Se dispone de un inventario gestionado por el departamento de Sistemas, que se realiza en la herramienta GLPI y que se mantiene actualizado, guardando en todo momento el responsable del activo.
op.exp.02	Configuración de Seguridad	L1	Se realiza una configuración básica de seguridad en los equipos de usuario (a través de un planchado de maquetas predefinido), pero no se cumplen los aspectos de seguridad requeridos, ni en no equipos de usuario ni en servidores.

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
op.exp.03	Gestión de la configuración	L1	No se cumplen correctamente la gestión de configuración ya que no disponen de funciones en dicho procedimiento del SGSI
op.exp.04	Mantenimiento	L3	No se dispone de un proceso de mantenimiento del equipamiento. En caso de necesidad, el departamento de sistemas provee de asistencia en caso de incidencia o petición de servicio si ello implica parches, actualizaciones, cambio de algún componente, etc.
op.exp.05	Gestión de cambios	L1	El departamento del Monitorización sigue correctamente el procedimiento. Los departamentos de seguridad no han sido incluidos en los procedimientos requeridos ni cumplen con la medida de protección.
op.exp.06	Protección frente a código dañino	L2	El actual Procedimiento de Respuesta a Virus no contempla el siguiente requisito: "Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo con las recomendaciones del fabricante."
op.exp.07	Gestión de incidentes	L3	Aunque en los distintos departamentos dentro del alcance disponen de la herramienta de gestión de incidentes Service Desk Plus, se echa en falta algún tipo de categorización que permita incluir incidentes de seguridad que puedan afectar a datos de carácter personal.
op.exp.08	Registro de la actividad de los usuarios	L1	No se puede evidenciar que se realice monitorización alguna en los equipos de usuario. Tampoco se ha podido evidenciar que se protejan los registros de actividad de administradores en Active Directory.
op.exp.08	Registro de la actividad de los usuarios	L0	No se revisan los registros de actividad en busca de patrones anormales.
op.exp.08	Registro de la actividad de los usuarios	**N/A**	
op.exp.09	Registro de la gestión de incidentes	L1	No se ha evidenciado procedimiento alguno que indique qué información debe salvaguardarse.
op.exp.10	Protección de los registros	N/A	
op.exp.11	Protección de claves criptográficas	L2	En NewCo se utiliza criptografía para la firma de correos electrónicos, cifrado de cintas. Además, existen repositorios de contraseñas que no disponen de medidas de seguridad adecuadas como contraseñas en hojas de cálculo
op.exp.11	Protección de claves criptográficas	L0	No existe un procedimiento de gestión de claves criptográficas que cumpla con los requisitos de la medida.
op.ext.1	Contratos y acuerdos de nivel de servicio	L3	Existe un procedimiento de Gestión de Suministradores que documenta los pasos a realizar antes y durante el suministro de servicios por la parte de proveedores. Se detalla en el documento las necesidades de determinar: - Alcance - Requisitos - Niveles de servicio - Revisiones

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
			- Desacuerdos e incumplimientos. Actualmente, no existe un cuadro de mandos que muestre indicadores de calidad o servicio por parte de los proveedores.
op.ext.2	Gestión diaria	L2	No se cumplen apartados a) y b) de la medida, relacionados directamente con la medida op.etx.1 Contratos y acuerdos de nivel de Servicio.
op.ext.9	Medios alternativos	L2	No se contempla documentación alguna o documento de continuidad que refleje, en caso de indisponibilidad del servicio, los medios alternativos para garantizar el provisionamiento de éste.
op.cont.1	Análisis de impacto	L1	En NewCo se disponen de Análisis de Impacto de Negocio. Cabe destacar que esta documentación es antigua y no se encuentra actualizada. Adicionalmente, no se disponen de BIAs realizados.
op.cont.2	Plan de continuidad	L1	Se dispone de un Plan de Continuidad del departamento del Sistemas internps, pero se encuentra desactualizado. Además, no se incluyen el resto de departamentos. Respecto a un ámbito técnico, el personal tiene conocimiento de cómo recuperar máquinas y servidores caídos, pero no se dispone de procedimientos o instrucciones técnicas que describan cómo debe hacerse.
op.cont.3	Pruebas periódicas	L0	No se dispone de un plan de pruebas que permita determinar si los Planes de de Continuidad son eficaces.
op.mon.1	Detección de intrusión	L2	No existen sistemas IDS/IPS. Existe un proyecto de monitorización y detección de intrusiones por parte del SOC de la Red de NewCo, pero no está activo actualmente.
op.mon.2	Sistema de métricas	L3	Se dispone de una Declaración de Aplicabilidad, que reúne los requisitos y controles del Anexo A de la norma ISO 27001. No se recopilan datos, pero se realizan auditorías internas y externas anualmente con el objetivo de conocer el grado de cumplimiento.
op.mon.2	Sistema de métricas	L2	No se miden los datos requeridos para Nivel MEDIO por parte del responsable
op.mon.2	Sistema de métricas	L2	No se miden los datos requeridos para Nivel ALTO por parte del responsable
mp.if.1	Áreas separadas y con control de acceso	L3	El equipamiento se instala en salas según las especificaciones de seguridad necesarias, pero no existe documentación que detalle qué tipo de zonas o áreas existen en la empresa y qué medidas de seguridad hay asociadas a cada una de ellas.
mp.if.2	Identificación de las personas	L3	Se registran las entradas a zonas en las que se almacena equipamiento o información sensible, pero no las salidas.
mp.if.3	Acondiciona miento de los locales	L3	Los locales que albergan el equipamiento que da soporte a los sistemas de información cuentan con los sistemas de refrigeración adecuados. Se evidencian sensores de temperatura o humedad en CPD, pero no existe una monitorización de la temperatura o humedad. Se desconoce cuál es el procedimiento a activar en caso de alcance de temperaturas que superen el umbral de trabajo normal del CPD.
mp.if.4	Energía eléctrica	L3	No se detectan insuficiencias al respecto

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
mp.if.4	Energía eléctrica	L3	Existe un Sistema de Alimentación Ininterrumpido. Se evidencia un checklist de procesos de apagado seguro en caso de emergencia. No se dispone de evidencia en la que se haya comprobado o resulte exitoso el proceso
mp.if.5	Protección frente a incendios	L3	No se detectan insuficiencias al respecto
mp.if.6	Protección frente a inundaciones	L3	No se detectan insuficiencias al respecto
mp.if.7	Registro de entrada y salida de equipamiento	L1	No se dispone de un proceso pormenorizado de entrada y salida de activos, aunque se realiza un control de estos.
mp.if.9	Instalaciones alternativas	L3	Actualmente existen instalaciones alternativas, aunque limitadas en lo que a cabida de empleados reubicados respecta. Adicionalmente, en caso de incidente en las instalaciones principales, los empleados pueden continuar realizando sus labores desde casa. No existe un plan de reubicación del personal en caso de incidente en instalaciones alternativas.
mp.per.1	Caracterización del puesto de trabajo	L2	El departamento de Personas no dispone de las necesidades y responsabilidades en materia de seguridad de la información de cada "job title" incumpliendo lo requerido por la medida. No se encuentran evidencias que muestren la existencia de fichas de puestos en el que se especifiquen las funciones de los distintos perfiles existentes en la organización.
mp.per.2	Deberes y obligaciones	L2	El personal de la entidad está sujeto a los deberes, responsabilidades y proceso disciplinarios reflejados en la Normativa de Seguridad de la entidad. Esta Normativa está desactualizada y no se ajusta a la realidad. Adicionalmente, no existe documentación alguna que abastezca las implicaciones de incumplimiento por parte de un tercero.
mp.per.3	Concienciación	L2	No se evidencia que los usuarios dispongan de conocimientos a la hora de notificar un incidente o actividad anómala.
mp.per.4	Formación	L2	Se realiza formación en seguridad de la información a la entrada de los empleados, no realizándose de forma continuada en el tiempo.
mp.per.9	Personal alternativo	L1	No se ha realizado un análisis de necesidades de personal alternativo a través de un Análisis de Impacto de Negocio.
mp.eq.1	Puesto de trabajo despejado	L1	Según la Normativa de Seguridad, el puesto de trabajo despejado es un punto fundamental del documento, pero se ha evidenciado la existencia de puestos de trabajo que han dejado fuera de horario laboral documentación confidencial
mp.eq.1	Puesto de trabajo despejado	L1	Se ha evidenciado información sensible almacenada en armarios que no están bajo llave fuera de horario laboral.
mp.eq.2	Bloqueo de puesto de trabajo	L0	En los departamentos que se circunscriben en el alcance no se realiza bloqueo de equipos tras un determinado tiempo de inactividad.

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
mp.eq.2	Bloqueo de puesto de trabajo	L0	Las sesiones no se cancelan pasado un cierto tiempo superior al anterior. Se alega que podría afectar a la operativa.
mp.eq.3	Protección de equipos portátiles	L1	Respecto a esta medida de protección, se consideran las siguientes insuficiencias: - Los discos duros de los ordenadores portátiles no están cifrados - Se requerirá de doble factor de autenticación para el acceso al equipo - Los usuarios que acceden a los equipos lo hacen con permisos de "admin" en vez de tipo "users" - Está habilitada la gestión remota de ordenadores de la organización
mp.eq.3	Protección de equipos portátiles	L0	No se dispone de dispositivos físicos/lógicos que permitan determinar si los equipos han sufrido violación o alteración alguna. Además, no se cifran los equipos que contienen información sensible.
mp.eq.9	Medios alternativos	L1	Actualmente no se han estudiado las necesidades tecnológicas respecto al parque tecnológico mínimo considerado como alternativo. Los equipos son de renting y se requiere de una solicitud previa del activo.
mp.com.1	Perímetro seguro	L4	No se detectan insuficiencias
mp.com.1	Perímetro seguro	L1	Actualmente, los sistemas de corta fuegos no están dispuestos en formato de doble capa. Adicionalmente no existe documentación en el sistema integrado de gestión en el que se defina la gestión o responsabilidad de dichas medidas de protección.
mp.com.2	Protección de la confidencialidad	L3	La VPN que emplea NewCo actualmente no hace uso de algoritmos acreditados por el CCN.
mp.com.2	Protección de la confidencialidad	L0	Las conexiones no se realizan con componentes certificados
mp.com.3	Protección de la autenticidad y de la integridad	L1	Se asegura la autenticidad de los extremos de comunicación durante el intercambio de información, aunque no se han realizado pruebas que demuestren protección frente a los puntos: 2. La inyección de información espuria. 3. El secuestro de la sesión por una tercera parte.
mp.com.3	Protección de la autenticidad y de la integridad	L1	NewCo dispone de mecanismos para proteger los intercambios de información cuando la comunicación transcurre fuera de la red de la organización. Sin embargo, no se utilizan algoritmos acreditados por el Centro Criptológico Nacional.
mp.com.3	Protección de la autenticidad y de la integridad		N/A
mp.com.4	Segregación de redes	L2	No se han segmentado las redes. Los departamentos del alcance están unidos a los sistemas generales de la entidad.

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
mp.com.9	Medios alternativos	L2	Aunque en lo que a comunicaciones respecta, se dispone de dos proveedores de comunicaciones y tecnologías diferentes, no se encuentra documentación al respecto sobre cómo activar la línea de backup.
mp.si.1	Etiquetado	L1	La información generada por la entidad no está siendo etiquetada correctamente según el esquema de clasificación de la Información que tiene definido.
mp.si.2	Criptografía	L2	Los departamentos que entran dentro del alcance del ENS no utilizan USB para el intercambio de información. Sistemas internos es el único departamento que los utiliza. El uso asociado es el de guardar las maquetas para planchar los equipos para empleados. Sin embargo, los equipos portátiles de usuarios no están debidamente cifrados. Las comunicaciones están cifradas a 128b o 256b según clientes.
mp.si.2	Criptografía	L2	No se contempla la adquisición de componentes o productos certificados por CCN en la documentación
mp.si.3	Custodia	L1	Se dispone de una normativa de uso de recursos corporativos en las que detalla lo está permitido y lo que no dentro de la entidad. Existen cajoneras de escritorio provistos de llave para su clausura durante los horarios no laborables. Se detectan deficiencias en este sentido ya que diversas cajoneras no están debidamente cerradas e incluyen información sensible.
mp.si.4	Transporte	L2	Los requisitos no están contemplados en la documentación, aunque se considera que el proceso se realiza de forma controlada por el personal.
mp.si.5	Borrado y destrucción	L1	No se dispone de una herramienta de borrado seguro. Los equipos y móviles se formatean con las opciones básicas del SO.
mp.si.5	Borrado y destrucción	L0	Actualmente no se destruyen los soportes, ya que son reciclados. No se dispone de herramienta de borrado seguro certificado por el CCN, Common Criteria o Lince.
mp.sw.1	Desarrollo de aplicaciones		N/A
mp.sw.2	Aceptación y puesta en servicio	L2	Generalmente, antes de que un sistema funcione en Producción se realiza la prueba asociada en un entorno de pruebas. No se ha evidenciado análisis de seguridad alguno durante la fase de pruebas en dicho entorno. Adicionalmente, no se establece documentación alguna en el Sistema Integrado de Gestión que contemple estos requerimientos
mp.sw.2	Aceptación y puesta en servicio	L1	En las aplicaciones que están en fase de entrada a producción no se realiza análisis de vulnerabilidades ni test de penetración.
mp.sw.2	Aceptación y puesta en servicio	L0	Actualmente no se realizan auditorias del código fuente y de integración en los procesos.
mp.info.1	Datos de carácter personal	L3	En general, NewCo en su actividad trata y almacena datos de carácter personal de distinta naturaleza. Además, desde abril de 2018 se ha llevado a cabo la adecuación al Reglamento General de Protección de Datos.
mp.info.2	Calificación de la información	L1	Actualmente la política no indica lo requerido por esta medida de seguridad. Adicionalmente, no se etiqueta la información debidamente según el esquema de clasificación adoptado por la entidad.

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
			Aunque existe una clasificación de la información, ésta no detalla las medidas de seguridad que se deben llevar a cabo para custodiarla.
mp.info.2	Calificación de la información	L1	Los procedimientos no indican de forma clara cómo realizar la calificación de la información correctamente
mp.info.3	Cifrado de la información	L1	Actualmente, la información cifrada es aquella transmitida a través de las comunicaciones y las que se almacenan en copia de seguridad. Sin embargo, la información almacenada en equipos no se realiza debidamente.
mp.info.4	Firma electrónica	L1	Solo un departamento utiliza firma para los correos electrónicos. Esta firma es autogenerada y se realiza a través de la aplicación Kleopatra. No está reconocida por las entidades certificadoras que exige el ENS.
mp.info.4	Firma electrónica	L1	Los certificados de firma no son cualificados ni se emplean algoritmos certificados por el CCN. Sin embargo, para la generación de certificados de firma se sigue lo indicado en el la guía CCN-STIC-955B
mp.info.4	Firma electrónica		N/A
mp.info.5	Sellos de tiempo		N/A
mp.info.6	Limpieza de documentos	L2	La limpieza de metadatos (eliminación de información de campos ocultos, comentarios, revisiones, versiones, etc.) de los documentos solo es realizada por un departamento, pero no el resto de los departamentos.
mp.info.9	Copias de seguridad (backup)	L1	Las copias de seguridad se realizan de forma periódica, almacenando información, configuraciones, bases de datos, etc. En caso de que la copia de seguridad no haya sido satisfactoria, se notifica a través de la herramienta de Service Desk +. Se descargan la información de Office 365 para hacer backup local vía VeemBackUp. Las aplicaciones on premise reciben copia en un NAS en Valencia. No se ha probado viabilidad o efectividad de su recuperación. No se realizan copias de toda la información dentro del alcance del ENS.
mp.s.1	Protección del correo electrónico (e-mail)	L2	El correo de la organización dispone protección en el correo, el cual implementa medidas de seguridad básicas, aunque no se cumplen los siguientes requisitos: "Limitaciones al uso como soporte de comunicaciones privadas." Protección frente "Código móvil de tipo «applet»."
mp.s.2	Protección de servicios y aplicaciones web	L1	Algunas aplicaciones publicadas no disponen de certificado SSL para el acceso en "HTTPS". La gestión de la configuración del cortafuegos es llevada a cabo por sistemas internos. No se dispone de sistemas de detección/protección frente a intrusiones que analicen el tráfico interno o hacia el exterior.
mp.s.2	Protección de servicios y aplicaciones web	L1	No se dispone de certificados cualificados en los servicios y aplicaciones publicas

ID	CONTROL	NIVEL MADUREZ	INSUFICIENCIAS
mp.s.8	Protección frente a la denegación de servicio	L0	En general, la capacidad de los sistemas están dimensionados para que se disponga de la posibilidad de atender la carga necesaria con la suficiente holgura. Esto se aplica a la mayoría de los sistemas. No existen tecnologías adicionales que permitan frenar ataques conocidos más allá de los cortafuegos y antivirus.
mp.s.8	Protección frente a la denegación de servicio	L0	No se dispone de herramientas anti-denegación de servicio salvo en Paterna, donde existe un cluster Fortinet (A/P) con capacidad de protección frente a DoS, pero no está activado. Tampoco existen herramientas que permitan la cancelación de ataques generados en la propia entidad.
mp.s.9	Medios Alternativos	L0	No se dispone de Plan de Continuidad de Negocio que defina las acciones, recursos y responsabilidades necesarias en caso de requerimiento de medidas alternativas.

ANEXOS

Anexo I: Política de Seguridad

APROBACIÓN Y ENTRADA EN VIGOR

El presente texto ha sido aprobado el día 20/03/2021 por la Dirección de NewCo.
Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación y hasta que la misma sea reemplazada por la aprobación de una nueva Política.

INTRODUCCIÓN

NewCo para alcanzar sus objetivos en el normal desarrollo de sus actividades, depende, en su gran mayoría, de los sistemas TIC (Tecnologías de información y Comunicaciones). Estos sistemas deben ser administrados con la debida diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar tanto a la disponibilidad, integridad o confidencialidad, así como autenticidad y trazabilidad de la información tratada o los servicios prestados.

El único fin de la seguridad de la información, y por tanto de la presente política, es garantizar la calidad de la información y la prestación continuada de los servicios, actuando de forma preventiva, supervisando las actividades diarias que se desarrollan en la organización y reaccionando con celeridad frente a los incidentes que puedan ocurrir.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial suficiente para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y de valor de la información y de los servicios.

Prevención, detección, reacción y recuperación

NewCo pone a disposición los recursos para evitar que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos y áreas deben implementar y aplicar al menos las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), a nivel de buenas prácticas las establecidas en la Norma ISO/IEC 27001 así como cualquier control adicional identificado a través

de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.
Para garantizar el cumplimiento de la política se debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Dado que, debido a incidentes, los servicios pueden verse rápidamente degradados, éstos deben de monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia; se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Para garantizar la disponibilidad de los servicios, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

ALCANCE

Este procedimiento es de aplicación a lo establecido en el documento Alcance y Contexto del SGSI.

VISIÓN Y MISIÓN

La compañía Newco es un master service provider y desea realizar una transformación, dada la tendencia actual que tienen las empresas de aprovisionar servidores de manera virtual en la nube (mayoritariamente en Amazon Web Services o en Microsot Azure, los líderes del mercado).

Newco es una compañía de doce empleados con una facturación de un millón de euros anuales. La empresa desea realizar un crecimiento orgánico para aumentar su facturación y experimentar un crecimiento en ventas.

El crecimiento orgánico es una estrategia de desarrollo de negocio que pasa por aumentar la producción para ampliar las ventas. Newco dispone de dos servidores físicos propios en un centro de datos que albergan máquinas virtuales de los más de sus cien clientes. Los servidores físicos están al límite de sus capacidades, por lo que un crecimiento orgánico solo puede darse si:

- Realizan una gran inversión en nuevos servidores físicos (aproximadamente 100.000 euros).
- Desean utilizar el modelo de suscripción en la nube de AWS o Microsoft Azure, un servicio de pago por uso de máquina virtual por hora (no es necesaria una inversión inicial).

Su modelo de negocio se verá afectado, ya que sus empleados tienen habilidades para la gestión de servidores físicos, pero no tienen ninguna experiencia en tecnología de computación en la nube. Es decir, no van a ser capaces de gestionar el producto que

venderán (máquinas virtuales en AWS o Microsoft Azure) debido a esa falta de habilidades.

El equipo directivo ha decidido no realizar una inversión en nueva maquinaria y optar por albergar los servidores de sus nuevos clientes en la nube. A medio plazo, se plantearán también la migración de los servidores físicos a la nube para optimizar costes.

MARCO NORMATIVO Y LEGAL

Esta Política se desarrollará conforme al marco normativo y legal aplicable en materia de seguridad, concretamente:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales y lo relativo a los mismos en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- En materia de protección de datos de carácter personal, Gedsa cumple con los dispuesto en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Normas de la Autoridad Nacional para la Protección de la Información Clasificada.
- UNE-EN ISO/IEC 27001, tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la Información y requisitos. Que contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Normativa interna

La presente política se desarrolla mediante un conjunto de documentos que forman la normativa interna del SGSI. Que se comprende de los siguientes ámbitos:

- Clasificación y etiquetado de la Información
- Seguridad en Explotación
- Seguridad en las Comunicaciones
- Gestión de Auditoria Interna de Seguridad
- Mejora Continua del Sistema de Gestión
- Gestión de la Seguridad en las Relaciones con Terceros
- Gestión de Activos y Soportes
- Análisis y Gestión de Riesgos
- Gestión de la Documentación del Sistema de Gestión

- Gestión de Copias de Seguridad y Restauración
- Gestión de Incidentes de Seguridad
- Gestión de Acceso Lógico de la Información
- Seguridad física y del entorno
- Adquisición, Desarrollo y Mantenimiento de Sistemas
- Gestión de la Continuidad del Servicio
- Gestión de Supervisión de Sistemas
- Firma electrónica, certificados y controles criptográficos
- Gestión de la seguridad en la relación con las personas

La normativa de seguridad estará a disposición de todos los miembros de la Organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

ORGANIZACIÓN DE LA SEGURIDAD

Comité

Con el fin de facilitar la implantación y gestión del proceso de seguridad en Gedsa, mediante la aprobación de la presente política, se aprueba también la formación de un **Comité de Seguridad de la Información** orientado a la gestión de la seguridad en la organización.

Este comité tiene la función de coordinar todas las funciones de seguridad de Gedsa, vela por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial. Asimismo, este comité se encarga de velar por el alineamiento de las actividades de seguridad y los objetivos de la organización.

Roles y responsabilidades

En el marco de cumplimiento del ENS y la ISO27001, y a fin de conformar la estructura de responsables en materia de seguridad, se han determinado los siguientes roles principales:

Responsable de la Información, representado por miembros de la dirección de la organización, como máximos responsables de la seguridad de la información.

Responsable de Seguridad de la Información, es el responsable de establecer y mantener las Políticas de Seguridad de la Información, estándares, directivas y procedimientos de la Organización y representado por el responsable del SGSI .

Responsable de Sistemas, responsable de la infraestructura de sistemas y comunicaciones.

Responsable de Instalaciones, representado por el representado por el director del área de intalaciones .

Adicionalmente, la atención, revisión y auditoría de la seguridad de los sistemas será realizada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

Procedimientos de designación

Los roles y responsabilidades en materia de seguridad de la información serán designados por la Dirección General y/o el Responsable de Seguridad de la Información, según la relación jerárquica de los perfiles afectados.

GESTIÓN DE RIESGOS

El procedimiento de Auditorías Internas asegura el alineamiento de las Tecnologías de la Información con las Políticas, Procedimientos y Legislación Aplicable.

Todos los sistemas sujetos a la presente Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando exista un cambio significativo en los sistemas de información
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, los responsables de la Información y Servicios establecerán una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

OBLIGACIONES DEL PERSONAL

Todas las personas de NewCo tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad que la desarrolla, así como desempeñar sus competencias con profesionalidad y ética.

Es responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados. Se establecerá un plan de formación y concienciación continua, en materia de seguridad de la información para atender a todas las personas de NewCo según su grado de responsabilidad.

TERCERAS PARTES

Cuando NewCo preste servicios o maneje información de terceros, se les hará participes de esta Política de Seguridad de la Información en la medida que se requiera, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad Corporativos y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando NewCo utilice servicios de terceros o ceda información a terceros, transmitirá también los requisitos de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información.)

NewCo únicamente cederá información a terceros que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos establecidos en su Política de Seguridad de la Información.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Asimismo, se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Se adoptarán las medidas oportunas en caso de incumplimiento de estos requerimientos, por parte de un tercero.

Anexo II: Declaración de Aplicabilidad (SOA)

Vistas las exigencias del Anexo II del ENS y las exigencias derivadas de los datos de carácter personal, se presenta a continuación una relación de las medidas que son de aplicación a cada Sistema descrito anteriormente.
Para ello se emplean las medidas detalladas en el Anexo II, enriquecidas o matizadas por características determinadas del sistema o exigencias derivadas del tratamiento de datos de carácter personal.
Cuando una medida requerida por el Anexo II en función de la valoración del sistema no se considere aplicable, esta no-aplicabilidad viene explicada en el campo observaciones. Cuando se recurre a medidas alternativas, se indica el motivo, así como las medidas que sustituye.
Las medidas se complementan con aquellas que son pertinentes a la vista del análisis de riesgos realizado, siempre respetando el mínimo exigible en virtud de la categoría del Sistema.

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	categoría	BÁSICO	Organizativo	Política de seguridad	org.1	Aplica	Si			x		
ENS	categoría	BÁSICO	Organizativo	Normativa de seguridad	org.2	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Organizativo	Procedimientos de seguridad	org.3	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Organizativo	Proceso de autorización	org.4	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Planificación	Análisis de riesgos	op.pl.1	Aplica	Si			x		
ENS	categoría	MEDIO	Planificación	Análisis de riesgos	op.pl.2	Aplica	Si			x		
ENS	categoría	ALTO	Planificación	Análisis de riesgos	op.pl.3	Aplica	Si			x		
ENS	categoría	BÁSICO	Planificación	Arquitectura de seguridad	op.pl.2	Aplica	Si	x		x		
ENS	categoría	MEDIO	Planificación	Arquitectura de seguridad	op.pl.2	Aplica	Si	x		x		
ENS	categoría	ALTO	Planificación	Arquitectura de seguridad	op.pl.2	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Planificación	Adquisición de nuevos componentes	op.pl.3	Aplica	Si			x		
ENS	D	MEDIO	Planificación	Dimensionamiento / Gestión de capacidades	op.pl.4	Aplica	Si			x		
ENS	categoría	ALTO	Planificación	Componentes certificados	op.pl.5	Aplica	Si			x		Medida compensatoria aplicada respecto a los Endpoint de Sophos, documentado en "Medidas Compensatorias - op.pl.5 Componentes certificados".
ENS	A T	BAJO	Control de acceso	Identificación	op.acc.1	Aplica	Si			x		
ENS	I C A T	BAJO	Control de acceso	Requisitos de acceso	op.acc.2	Aplica	Si	x		x		

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	I C A T	MEDIO	Control de acceso	Segregación de funciones y tareas	op.acc.3	Aplica	Si			x		
ENS	I C A T	BAJO	Control de acceso	Proceso de gestión de derechos de acceso	op.acc.4	Aplica	Si	x		x		
ENS	I C A T	BAJO	Control de acceso	Mecanismo de autenticación	op.acc.5	Aplica	Si	x		x		
ENS	I C A T	MEDIO	Control de acceso	Mecanismo de autenticación	op.acc.5	Aplica	Si	x		x		
ENS	I C A T	ALTO	Control de acceso	Mecanismo de autenticación	op.acc.5	Aplica	Sí *	x		x		Medida compensatoria aplicada para sistema de Sistemas Internos. Documentado en "Medidas Compensatorias - op.acc.5 Mecanismo de autenticación"
ENS	I C A T	BAJO	Control de acceso	Acceso local (local logon)	op.acc.6	Aplica	Si	x		x		
ENS	I C A T	MEDIO	Control de acceso	Acceso local (local logon)	op.acc.6	Aplica	Si	x		x		
ENS	I C A T	ALTO	Control de acceso	Acceso local (local logon)	op.acc.6	Aplica	Si	x		x		
ENS	I C A T	BAJO	Control de acceso	Acceso remoto (remote login)	op.acc.7	Aplica	Si	x		x		
ENS	I C A T	MEDIO	Control de acceso	Acceso remoto (remote login)	op.acc.7	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Explotación	Inventario de activos	op.exp.01	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Explotación	Configuración de Seguridad	op.exp.02	Aplica	Si	x		x		
ENS	categoría	MEDIO	Explotación	Gestión de la configuración	op.exp.03	Aplica	Si			x		
ENS	categoría	BÁSICO	Explotación	Mantenimiento	op.exp.04	Aplica	Si	x		x		

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	categoría	MEDIO	Explotación	Gestión de cambios	op.exp.05	Aplica	Si			x		
ENS	categoría	BÁSICO	Explotación	Protección frente a código dañino	op.exp.06	Aplica	Si	x		x		
ENS	categoría	MEDIO	Explotación	Gestión de incidentes	op.exp.07	Aplica	Si			x		
ENS	T	BAJO	Explotación	Registro de la actividad de los usuarios	op.exp.08	Aplica	Si	x		x		
ENS	T	MEDIO	Explotación	Registro de la actividad de los usuarios	op.exp.08	Aplica	Si	x		x		
ENS	T	ALTO	Explotación	Registro de la actividad de los usuarios	op.exp.08	Aplica	Sí *			x		
ENS	categoría	MEDIO	Explotación	Registro de la gestión de incidentes	op.exp.09	Aplica	Si			x		
ENS	T	ALTO	Explotación	Protección de los registros	op.exp.10	Aplica	Sí *			x		
ENS	categoría	BÁSICO	Explotación	Protección de claves criptográficas	op.exp.11	Aplica	Si			x		
ENS	categoría	MEDIO	Explotación	Protección de claves criptográficas	op.exp.11	Aplica	Si			x		
ENS	categoría	MEDIO	Servicios externos	Contratos y acuerdos de nivel de servicio	op.ext.1	Aplica	Si	x		x		
ENS	categoría	MEDIO	Servicios externos	Gestión diaria	op.ext.2	Aplica	Si	x		x		
ENS	D	ALTO	Servicios externos	Medios alternativos	op.ext.9	Aplica	Si			x		
ENS	D	MEDIO	Continuidad de negocio	Análisis de impacto	op.cont.1	Aplica	Si	x		x		
ENS	D	ALTO	Continuidad de negocio	Plan de continuidad	op.cont.2	Aplica	Si	x		x		
ENS	D	ALTO	Continuidad de negocio	Pruebas periódicas	op.cont.3	Aplica	Si	x		x		
ENS	categoría	MEDIO	Monitorización del sistema	Detección de intrusión	op.mon.1	Aplica	Si	x		x		

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	categoría	BAJO	Monitorización del sistema	Sistema de métricas	op.mon.2	Aplica	Si	x		x		
ENS	categoría	MEDIO	Monitorización del sistema	Sistema de métricas	op.mon.2	Aplica	Si	x		x		
ENS	categoría	ALTO	Monitorización del sistema	Sistema de métricas	op.mon.2	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Protección de las instalaciones e infraestructuras	Áreas separadas y con control de acceso	mp.if.1	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Protección de las instalaciones e infraestructuras	Identificación de las personas	mp.if.2	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de las instalaciones e infraestructuras	Acondicionamiento de los locales	mp.if.3	Aplica	Si	x		x		
ENS	D	BAJO	Protección de las instalaciones e infraestructuras	Energía eléctrica	mp.if.4	Aplica	Si	x		x		
ENS	D	MEDIO	Protección de las instalaciones e infraestructuras	Energía eléctrica	mp.if.4	Aplica	Si	x		x		
ENS	D	BAJO	Protección de las instalaciones e infraestructuras	Protección frente a incendios	mp.if.5	Aplica	Si	x		x		
ENS	D	MEDIO	Protección de las instalaciones e infraestructuras	Protección frente a inundaciones	mp.if.6	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Protección de las instalaciones e infraestructuras	Registro de entrada y salida de equipamiento	mp.if.7	Aplica	Si	x		x		
ENS	D	ALTO	Protección de las instalaciones e infraestructuras	Instalaciones alternativas	mp.if.9	Aplica	Si			x		
ENS	categoría	MEDIO	Gestión del personal	Caracterización del puesto de trabajo	mp.per.1	Aplica	Si			x		
ENS	categoría	BÁSICO	Gestión del personal	Deberes y obligaciones	mp.per.2	Aplica	Si	x		x		

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	categoría	BÁSICO	Gestión del personal	Concienciación	mp.per.3	Aplica	Si	x		x		
ENS	categoría	BÁSICO	Gestión del personal	Formación	mp.per.4	Aplica	Si	x		x		
ENS	D	ALTO	Gestión del personal	Personal alternativo	mp.per.9	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de los equipos	Puesto de trabajo despejado	mp.eq.1	Aplica	Si			x		
ENS	categoría	MEDIO	Protección de los equipos	Puesto de trabajo despejado	mp.eq.1	Aplica	Si			x		
ENS	A	MEDIO	Protección de los equipos	Bloqueo de puesto de trabajo	mp.eq.2	Aplica	Si	x		x		
ENS	A	ALTO	Protección de los equipos	Bloqueo de puesto de trabajo	mp.eq.2	Aplica	Sí *			x		
ENS	categoría	BÁSICO	Protección de los equipos	Protección de equipos portátiles	mp.eq.3	Aplica	Si	x		x		
ENS	categoría	ALTO	Protección de los equipos	Protección de equipos portátiles	mp.eq.3	Aplica	Si	x		x		
ENS	D	MEDIO	Protección de los equipos	Medios alternativos	mp.eq.9	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de las comunicaciones	Perímetro seguro	mp.com.1	Aplica	Si	x		x		
ENS	categoría	ALTO	Protección de las comunicaciones	Perímetro seguro	mp.com.1	Aplica	Si	x		x		
ENS	C	MEDIO	Protección de las comunicaciones	Protección de la confidencialidad	mp.com.2	Aplica	Si	x		x		
ENS	C	ALTO	Protección de las comunicaciones	Protección de la confidencialidad	mp.com.2	Aplica	Si	x		x		
ENS	I A	BAJO	Protección de las comunicaciones	Protección de la autenticidad y de la integridad	mp.com.3	Aplica	Si	x		x		
ENS	I A	MEDIO	Protección de las comunicaciones	Protección de la autenticidad y de la integridad	mp.com.3	Aplica	Si	x		x		
ENS	I A	ALTO	Protección de las comunicaciones	Protección de la autenticidad y de la integridad	mp.com.3	Aplica	Sí *			x		

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	categoría	ALTO	Protección de las comunicaciones	Segregación de redes	mp.com.4	Aplica	Si			x		
ENS	D	ALTO	Protección de las comunicaciones	Medios alternativos	mp.com.9	Aplica	Si	x		x		
ENS	C	BAJO	Protección de los soportes de información	Etiquetado	mp.si.1	Aplica	Si			x		
ENS	I C	MEDIO	Protección de los soportes de información	Criptografía	mp.si.2	Aplica	Si			x		
ENS	I C	ALTO	Protección de los soportes de información	Criptografía	mp.si.2	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de los soportes de información	Custodia	mp.si.3	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de los soportes de información	Transporte	mp.si.4	Aplica	Si			x		
ENS	C	BAJO	Protección de los soportes de información	Borrado y destrucción	mp.si.5	Aplica	Si	x		x		
ENS	C	MEDIO	Protección de los soportes de información	Borrado y destrucción	mp.si.5	Aplica	Si	x		x		
ENS	categoría	MEDIO	Protección de las aplicaciones informáticas	Desarrollo de aplicaciones	mp.sw.1	N/A	-				Dentro de los departamentos circunscritos en el alcance, no se realiza desarrollo.	
ENS	categoría	BÁSICO	Protección de las aplicaciones informáticas	Aceptación y puesta en servicio	mp.sw.2	Aplica	Si			x		
ENS	categoría	MEDIO	Protección de las aplicaciones informáticas	Aceptación y puesta en servicio	mp.sw.2	Aplica	Si			x		

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	categoría	ALTO	Protección de las aplicaciones informáticas	Aceptación y puesta en servicio	mp.sw.2	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de la información	Datos de carácter personal	mp.info.1	Aplica	Si			x		
ENS	C	BAJO	Protección de la información	Calificación de la información	mp.info.2	Aplica	Si			x		
ENS	C	MEDIO	Protección de la información	Calificación de la información	mp.info.2	Aplica	Si			x		
ENS	C	ALTO	Protección de la información	Cifrado de la información	mp.info.3	Aplica	Si	x	x	x		
ENS	I A	BAJO	Protección de la información	Firma electrónica	mp.info.4	Aplica	Si			x		
ENS	I A	MEDIO	Protección de la información	Firma electrónica	mp.info.4	Aplica	Si			x		
ENS	I A	ALTO	Protección de la información	Firma electrónica	mp.info.4	Aplica	Sí *			x		
ENS	T	ALTO	Protección de la información	Sellos de tiempo	mp.info.5	Aplica	Sí *			x		
ENS	C	BAJO	Protección de la información	Limpieza de documentos	mp.info.6	Aplica	Si			x		
ENS	D	BAJO	Protección de la información	Copias de seguridad (backup)	mp.info.9	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de los servicios	Protección del correo electrónico (e-mail)	mp.s.1	Aplica	Si			x		
ENS	categoría	BÁSICO	Protección de los servicios	Protección de servicios y aplicaciones web	mp.s.2	Aplica	Si			x		
ENS	categoría	ALTO	Protección de los servicios	Protección de servicios y aplicaciones web	mp.s.2	Aplica	Si			x		
ENS	D	MEDIO	Protección de los servicios	Protección frente a la denegación de servicio	mp.s.8	Aplica	Si	x		x		
ENS	D	ALTO	Protección de los servicios	Protección frente a la denegación de servicio	mp.s.8	Aplica	Si	x		x		

NORMATIVA	DIMENSIÓN	NIVEL	DOMINIO	CONTROL	ID	APLICACIÓN	IMPLEM.	INCLUSIONES			JUSTIFICACIÓN EXCLUSIÓN	COMPENSATORIA
								AARR	Contract.	Estrategia		
ENS	D	ALTO	Protección de los servicios	Medios Alternativos	mp.s.9	Aplica	Si			x		

Anexo III Plan de mejora seguridad

Una vez identificadas las insuficiencias y los riesgos dentro del proyecto de adecuación, se proponen a continuación una serie de medidas destinadas a subsanar las deficiencias detectadas. Según la Guía CCN-STIC-804 de implantación del ENS, para los niveles altos de los subsistemas a certificar, se espera un nivel de madurez L4, que sea Gestionado y medible.

Se muestra a continuación, el plan de mejora de la seguridad para poder dar cumplimiento a las diferentes medidas de seguridad que son de aplicabilidad a los sistemas de NewCo:

ID	CONTROL	PLAN DE MEJORA	Fecha Inicio y Fin
org.1	Política de seguridad	Aunque NewCo dispone actualmente de una Política de Seguridad de la Información que cumple con los requisitos de la ISO/IEC 27001, la organización debe actualizar dicha documentación, incluyendo los siguientes requisitos detallados en el punto de insuficiencias respectivo.	06-Mayo/20-Septiembre
org.2	Normativa de seguridad	NewCo incluye en su documentación del Sistema Integrado de Gestión una Normativa de Seguridad, ésta se debe rediseñar, añadiendo los deberes y derechos de los empleados y actualizándola según los requisitos del Esquema Nacional de Seguridad [org.2]	06-Mayo/20-Septiembre
org.3	Procedimientos de seguridad	Se ha de actualizar la normativa y otra documentación de seguridad relativa al Sistema de Gestión, actualizándola a la casuística real de la entidad.	06-Mayo/20-Septiembre
org.4	Proceso de autorización	Se han de actualizar los procedimientos y normas, incluyendo las fases de autorización necesarias.	06-Mayo/20-Septiembre
op.pl.1	Análisis de riesgos	No se han detectado mejora necesaria	
op.pl.1	Análisis de riesgos	No se han detectado mejora necesaria	
op.pl.1	Análisis de riesgos	No se han detectado mejora necesaria	
op.pl.2	Arquitectura de seguridad	Se debe definir un documento de Arquitectura de Seguridad que incluya todos los requisitos de la medida de protección y que muestre, de forma resumida, los esquemas de red, perímetro de seguridad, y diferentes clasificaciones de zonas de NewCo, entre otros.	06-Mayo/20-Septiembre
op.pl.2	Arquitectura de seguridad	Se debe definir un documento de Arquitectura de Seguridad que incluya todos	06-Mayo/20-

		los requisitos de la medida de protección y que muestre, de forma resumida, los esquemas de red, perímetro de seguridad, y diferentes clasificaciones de zonas de NewCo, entre otros.	Septiembre
op.pl.2	Arquitectura de seguridad	Se debe definir un documento de Arquitectura de Seguridad que incluya todos los requisitos de la medida de protección y que muestre, de forma resumida, los esquemas de red, perímetro de seguridad, y diferentes clasificaciones de zonas de NewCo, entre otros.	06-Mayo/20-Septiembre
op.pl.3	Adquisición de nuevos componentes	Se debe diseñar un documento que indique cómo se debe realizar el proceso de adquisición de nuevos componentes (p. ej.: adquisición de un servidor, firewall, antivirus, cinta de backup, etc.). Este procedimiento debe garantizar que las adquisiciones estén alineadas con la arquitectura de seguridad definida	06-Mayo/20-Septiembre
op.pl.4	Dimensionamiento / Gestión de capacidades	Este procedimiento existe para el departamento de Sistemas internos. Debe ser ampliado a los otros departamentos que se incluyen en el alcance.	06-Mayo/20-Septiembre
op.pl.5	Componentes certificados	Es necesario realizar una migración de los componentes no certificados a componentes certificados. Para ello, se han de tener en cuenta, por el siguiente orden, los repositorios de componentes certificados del CCN, COMMONCRITERIA, LINCE (sistemas de nivel medio). 1. Priorizar qué componentes son los que deben estar certificados (todos es imposible lograrlo). 2. Analizar si se encuentran en la Guía CCN-STIC 105 Catálogo de productos de seguridad de las TIC o la web https://oc.ccn.cni.es/index.php/es/productos-certificados/productos-certificados/categoria-de-producto/15-herramientas-anti-virus?search=&order=i.created&dir=desc&cm=0#tlb a. En caso de que esté, adelante. b. En caso de que no esté, mirar en Common Criteria y en última instancia, en LINCE.	06-Mayo/20-Septiembre

		c. En caso de que no esté tampoco, utilizar Guía CCN-STIC 140 Taxonomía de referencia para productos de seguridad TIC para realizar test internos (se dispone en NewCo) como medida compensatoria. 3. En caso de que el punto 2 no se pueda abordar, realizar análisis de riesgos de proporcionalidad (que sean las mínimas veces posibles).	
op.acc.1	Identificación	Se ha de actualizar la documentación relativa a los controles de acceso lógicos. Adicionalmente, se deben separar usuarios de administradores, siendo éstos nominales, permitiendo en todo momento conocer la trazabilidad de la actividad en los Sistemas de Información.	06-Mayo/20-Septiembre
op.acc.2	Requisitos de acceso	Se han de definir los requisitos de acceso para los diferentes recursos de la entidad. Además de detallar quién es el propietario de cada uno de los recursos, se ha de detallar el proceso de autorización para éstos.	06-Mayo/20-Septiembre
op.acc.3	Segregación de funciones y tareas	Se deben separar los roles de administradores y usuarios en los equipos locales, de forma que se impida el abuso de privilegios de los usuarios autorizados. Principalmente, se ha de disponer de documentación que permita plasmar las siguientes premisas: - nadie puede autorizarse a sí mismo - los desarrolladores no pueden modificar datos de explotación - los desarrolladores no pueden pasar software a explotación - los desarrolladores no pueden configurar software en explotación - los operadores ni desarrollan software ni pueden modificar los desarrollos - los usuarios ni desarrollan ni pueden modificar los desarrollos - los usuarios ni configuran ni pueden modificar la configuración	06-Mayo/20-Septiembre
op.acc.4	Proceso de gestión de derechos de acceso	Se deben separar correctamente los recursos de forma que se impida el acceso a usuarios no autorizados, atendiendo al principio de mínimo privilegio. Además, se debe: 1. Revisar los procedimientos de alta/baja usuarios y autorización a recursos con el objetivo de que se incluyen las necesidades	06-Mayo/20-Septiembre

		de la medida. 2. Para colaboradores externos, deben asignarse permisos con fecha fin, de forma que, finalizada la relación contractual, el acceso quede invalidado. 3. Realizar revisiones periódicas de los permisos de acceso, con el objetivo de descartar accesos no permitidos.	
op.acc.5	Mecanismo de autenticación	Actualmente NewCo dispone de mecanismos diversos de autenticación. Aun así, se requiere de la adopción de diferentes medidas para el acceso a los recursos, como por ejemplo la habilitación de un repositorio de contraseñas debidamente protegido.	06-Mayo/20-Septiembre
op.acc.5	Mecanismo de autenticación	Se ha de establecer doble autenticación en: - Office 365 (Correo y Sharepoint) - Administración de SOPHOS - Administración de BARRACUDA - Proxies con certificado para: - ZABBIX - Service Desk + - Qradar - The Hive - Citrix -Syspass - Equipos de usuario (bitlocker y acceso a sesión local o acceso biométrico)	06-Mayo/20-Septiembre
op.acc.5	Mecanismo de autenticación	Se debe activar la suspensión de credenciales pasado un periodo determinado.	06-Mayo/20-Septiembre
op.acc.6	Acceso local (local logon)	Se han de bloquear los intentos de acceso fallidos. Se implementará un "disclaimer" o ventana donde se le informará al usuario de las obligaciones en su acceso	06-Mayo/20-Septiembre
op.acc.6	Acceso local (local logon)	Se debe implementar un aviso o disclaimer que muestre al usuario el ultimo acceso realizado y la ubicación.	06-Mayo/20-Septiembre
op.acc.6	Acceso local (local logon)	No se limita el horario de uso, debido a que el servicio es 24x7 y el equipo operativo disponen de horarios de guardia. Se debe analizar la necesidad de puntos de control en la renovación de autenticación del usuario.	06-Mayo/20-Septiembre

op.acc.7	Acceso remoto (remote login)	Se ha de obligar al usuario que accede remotamente a usar conexión cifrada y segura (VPN).	06-Mayo/20-Septiembre
op.acc.7	Acceso remoto (remote login)	Se ha de incluir en la documentación proporcionada al usuario, lo que se está autorizado a hacer en remoto	06-Mayo/20-Septiembre
op.exp.01	Inventario de activos	Se han de actualizar los inventarios de activos de la entidad. Además, se recomienda unificarlos en un mismo repositorio con el objetivo de garantizar la integridad de la información.	06-Mayo/20-Septiembre
op.exp.02	Configuración de Seguridad	Se debe documentar un procedimiento de bastionado de equipos correctamente	06-Mayo/20-Septiembre
op.exp.03	Gestión de la configuración	Se ha de definir los criterios y configuraciones por defecto de los equipos, sistemas, servidores, etc. determinando funcionalidades mínimas y criterios para la notificación de incidentes.	06-Mayo/20-Septiembre
op.exp.04	Mantenimiento	Se debe detallar en la documentación, los detalles del ciclo de vida del equipamiento físico y lógico.	06-Mayo/20-Septiembre
op.exp.05	Gestión de cambios	La gestión de cambios, que atañe únicamente al departamento del Sistemas Internos, se ha de ampliar y contemplar en el resto de departamentos. Se debe actualizar la documentación existente, incluyendo sobre todo la notificación y comunicación de los cambios a las partes afectadas.	06-Mayo/20-Septiembre
op.exp.06	Protección frente a código dañino	Se ha de establecer un proceso de comunicación de anomalías y concienciar al personal, estableciendo una formación para la notificación de incidentes.	06-Mayo/20-Septiembre
op.exp.07	Gestión de incidentes	La herramienta de *ticketing* ha de poder reflejar las diferencias entre eventos, incidencias e incidentes de seguridad.	06-Mayo/20-Septiembre
op.exp.08	Registro de la actividad de los usuarios	Para garantizar la protección de la trazabilidad, se debe: 1. Activar los modos de auditoría para usuarios administradores del Active Directory. 2. Definir y activar registros de auditoría en servidores.	06-Mayo/20-Septiembre

		3. Revisar los registros / eventos. 4. Disponer de herramienta de monitorización/recolección de eventos.	
op.exp.08	Registro de la actividad de los usuarios	Se debe establecer un procedimiento de control de acceso lógico que defina el protocolo de permisos que debe recibir un empleado, según las necesidades de su puesto de trabajo.	06-Mayo/20-Septiembre
op.exp.08	Registro de la actividad de los usuarios	N/A	
op.exp.09	Registro de la gestión de incidentes	Se debe implementar un procedimiento de gestión de acceso lógico que aúne y se relacione con la gestión de incidentes.	06-Mayo/20-Septiembre
op.exp.10	Protección de los registros	N/A	
op.exp.11	Protección de claves criptográficas	Se ha de definir un documento que indique el procedimiento sobre: - La generación de claves criptográficas - El transporte de éstas - La ejecución y uso - El borrado y destrucción	06-Mayo/20-Septiembre
op.exp.11	Protección de claves criptográficas	Se ha de establecer la generación y custodia de claves criptográficas recojan los requisitos necesarios y que incluyan la adquisición de estos a través de medios acreditados.	06-Mayo/20-Septiembre
op.ext.1	Contratos y acuerdos de nivel de servicio	Aunque existe documentación relacionada con la gestión de proveedores, se ha de añadir la necesidad de establecer indicadores de calidad o servicio por parte de éstos.	06-Mayo/20-Septiembre
op.ext.2	Gestión diaria	Se ha de detallar un procedimiento documentado que defina la periodicidad de medición del cumplimiento de las obligaciones de los servicios, el responsable asociado de dicha medición y los protocolo o sanciones en caso de incumplimiento o degradación del servicio contratado.	06-Mayo/20-Septiembre
op.ext.9	Medios alternativos	Se debe documentar un procedimiento e implantar un Plan de Continuidad de Negocio referente a los servicios que provee NewCo dentro del Alcance. Una vez realizado, se ha de poder garantizar la provisión del servicio.	06-Mayo/20-Septiembre
op.cont.1	Análisis de impacto	Se ha de realizar un Análisis de Impacto de Negocio en los diferentes departamentos del Alcance, con el objetivo de determinar las necesidades de recuperación en caso de caída.	06-Mayo/20-Septiembre

op.cont. 2	Plan de continuidad	Se debe desarrollar un Plan de Continuidad de Negocio en el que se identifiquen y describan los servicios que proveen los departamentos del Alcance y las necesidades asociadas en caso de caída del servicio. Se deben definir escenarios de riesgo que permitan a la entidad activar contingencia en caso de desastre disruptivo.	06-Mayo/20-Septiembre
op.cont. 3	Pruebas periódicas	Se ha de establecer un Plan de Pruebas de Continuidad, en el que se planifiquen en un calendario las diferentes pruebas que se consideren necesarias según los Escenarios de Riesgo identificados en el Plan de Continuidad de Negocio.	06-Mayo/20-Septiembre
op.mon. 1	Detección de intrusión	Se debe monitorizar la red que se adscribe en el alcance. Se propone que el departamento del SOC proporcione estos servicios. Para ello se ha de: - Monitorizar los activos a través de la instalación de un NIDS y un HIDS. - Implantar agentes en servidores de NewCo. - Generar informes de resultados según periodicidad establecida. -Configurar activos para que se realicen escáner de vulnerabilidades en busca de debilidades.	06-Mayo/20-Septiembre
op.mon. 2	Sistema de métricas	Se debe formalizar el proceso de generación de indicadores, debiendo estar aprobado un conjunto de indicadores, indicando para cada uno de ellos: - el objetivo que se pretende medir - el responsable del indicador - el origen de la información - el procedimiento de recogida y tratamiento de datos (mediciones) - la frecuencia de recogida de datos - el método de elaboración de indicadores a partir de las medidas - la elaboración de indicadores agregados a partir de otros indicadores - los criterios de valoración del indicador a efectos de reaccionar y tomar decisiones	06-Mayo/20-Septiembre
op.mon. 2	Sistema de métricas	Realizar mediciones de forma que se almacenen los siguientes datos: – Número de incidentes de seguridad tratados. – Tiempo empleado para cerrar el 50% de los	06-Mayo/20-Septiembre

		incidentes. – Tiempo empleado para cerrar el 90% de los incidentes.	
op.mon.2	Sistema de métricas	Medir la eficiencia de las medidas de seguridad aplicadas y del Sistema de Gestión de NewCo de forma que se pueda estimar en recursos y presupuestos los proyectos establecidos.	06-Mayo/20-Septiembre
mp.if.1	Áreas separadas y con control de acceso	Detallar en un documento o norma lo que se puede hacer o no en las diferentes zonas de la entidad.	06-Mayo/20-Septiembre
mp.if.2	Identificación de las personas	Se ha de implantar un mecanismo de autenticación biométrico que permita identificar a las personas entrantes y salientes de las zonas que almacenen activos de información catalogados como sensibles.	06-Mayo/20-Septiembre
mp.if.3	Acondicionamiento de los locales	Relacionado con el Plan de Continuidad de Negocio, se ha de definir un procedimiento a seguir en caso de que los recursos que permiten el correcto acondicionamiento de los locales caigan o fallen los suministros asociados.	06-Mayo/20-Septiembre
mp.if.4	Energía eléctrica	Se recomienda realizar un estudio de las necesidades de potencia eléctrica	06-Mayo/20-Septiembre
mp.if.4	Energía eléctrica	Se han de realizar las pruebas necesarias con el objetivo de esclarecer la efectividad del proceso de apagado seguro de los procesos en caso de caída de la red eléctrica.	06-Mayo/20-Septiembre
mp.if.5	Protección frente a incendios	Se recomienda la implantación de sensores de temperatura que notifiquen debidamente al personal técnico. Se recomienda además la realización de acciones formativas o simulacros para este tipo de incidentes.	06-Mayo/20-Septiembre
mp.if.6	Protección frente a inundaciones	Se recomienda realizar un estudio de la ubicación física de las áreas frente a las amenazas sobre inundaciones.	06-Mayo/20-Septiembre
mp.if.7	Registro de entrada y salida de equipamiento	Se recomienda la documentación de un procedimiento que indique los pasos a seguir en el caso de que determinados activos que contenga información tengan que salir de las instalaciones. Se deben establecer las medidas de seguridad asociadas para los	06-Mayo/20-Septiembre

		dispositivos en su tránsito por las diferentes zonas de NewCo.	
mp.if.9	Instalaciones alternativas	Se debe establecer y mantener actualizado un Plan de Emergencias que a su vez disponga de un Plan de Reubicación del Personal. Se recomienda llevar a cabo simulacros que permitan determinar las necesidades, incidencias, oportunidades de mejoras, etc. y aplicar la mejora continua.	06-Mayo/20-Septiembre
mp.per.1	Caracterización del puesto de trabajo	Se ha de desarrollar una política o normativa documentada que contenga: - la caracterización de cada puesto de trabajo en materia de seguridad. - la definición de las responsabilidades relacionadas con cada puesto de trabajo basándose en el análisis de riesgos en la medida en que afecta a cada puesto de trabajo.	06-Mayo/20-Septiembre
mp.per.2	Deberes y obligaciones	Se han de incluir los deberes y responsabilidades por parte de terceros en la Normativa de Seguridad Corporativa. Dichas normativas, junto con las políticas, deben ser comunicadas a terceros	06-Mayo/20-Septiembre
mp.per.3	Concienciación	Se ha de documentar un Plan de Concienciación que indique las necesidades de NEWCO en lo que percepción, conocimiento y percepción respecta, dentro del ámbito de la seguridad de la información, haciendo buen uso de los sistemas de información y conociendo el flujo a llevar a cabo para la gestión de incidentes.	06-Mayo/20-Septiembre
mp.per.4	Formación	Se recomienda ampliar la formación de los empleados en seguridad de la información más allá de su etapa o fase inicial, ayudando a mantener los conocimientos adquiridos actualizados.	06-Mayo/20-Septiembre
mp.per.9	Personal alternativo	Se ha de contemplar dentro del Plan de Continuidad de Negocio.	06-Mayo/20-Septiembre
mp.eq.1	Puesto de trabajo despejado	Aunque este punto se relacione con la Concienciación y la Formación, actualmente en NEWCO, el personal ha de recibir formación respecto a cómo habilitar un puesto de trabajo despejado.	06-Mayo/20-Septiembre
mp.eq.1	Puesto de trabajo despejado	A la finalización del horario laboral, los empleados deberán dejar un puesto de	06-Mayo/20-

		trabajo seguro, sin información sensible en lugares visibles y manteniendo toda información en los armarios o cajoneras habilitadas con cierre.	Septiembre
mp.eq.2	Bloqueo de puesto de trabajo	Se han de habilitar las medidas pertinentes de forma que los equipos se bloqueen llegados los 5 o 10 minutos, según decisión del Responsable de Seguridad.	06-Mayo/20-Septiembre
mp.eq.2	Bloqueo de puesto de trabajo	Se han de habilitar las medidas pertinentes de forma que los equipos cierren las sesiones superado un tiempo determinado, según decisión del Responsable de Seguridad.	06-Mayo/20-Septiembre
mp.eq.3	Protección de equipos portátiles	Para mantener la protección de los equipos fuera de las instalaciones, se debe: - Cifrar equipos portátiles y dispositivos móviles. - En caso de robo, proceder al borrado remoto. - Acceder a los Sistemas de Información a través de redes privadas protegidas (VPN) Las medidas citadas anteriormente, se pueden gestionar a través del uso de un MDM (Mobile Device Manager)	06-Mayo/20-Septiembre
mp.eq.3	Protección de equipos portátiles	Valorar e implantar la inclusión de dispositivos físicos (p.e. pegatinas) o lógicos con software de protección que detecte cambios de configuración.	06-Mayo/20-Septiembre
mp.eq.9	Medios alternativos	Relacionado con el Plan de Continuidad de Negocio, se han de establecer y definir los activos mínimos necesarios por parte de los departamentos y áreas para la provisión de servicios.	06-Mayo/20-Septiembre
mp.com.1	Perímetro seguro	No se requiere de acciones de mejora	
mp.com.1	Perímetro seguro	Se ha de planificar la implantación de un conjunto de cortafuegos de forma que se permita acceder a los recursos corporativos de forma segura.	06-Mayo/20-Septiembre
mp.com.2	Protección de la confidencialidad	No se requiere de acciones de mejora	
mp.com.2	Protección de la confidencialidad	Se ha de implantar un producto certificado como método de acceso desde fuera de las instalaciones de la entidad.	06-Mayo/20-Septiembre
mp.com.3	Protección de la autenticidad y de la integridad	Se recomienda desarrollar y aplicar una política o normativa documentada que indique: - el uso de dispositivos hardware en el	06-Mayo/20-Septiembre

		establecimiento y utilización de la VPN. En caso de no utilización de dispositivos hardware debe estar debidamente acreditado y aprobado por el responsable. - el uso de productos certificados (en relación con [op.pl.5]) o si está aprobado por el responsable.	
mp.com.3	Protección de la autenticidad y de la integridad	Ver punto anterior	06-Mayo/20-Septiembre
mp.com.3	Protección de la autenticidad y de la integridad	N/A	
mp.com.4	Segregación de redes	Se ha de establecer un esquema de red que permita segmentar las diferentes redes de la entidad separando los sistemas de información del alcance de las demás redes, con el objetivo aplicar una mayor capa de protección.	06-Mayo/20-Septiembre
mp.com.9	Medios alternativos	Se han de realizar pruebas de funcionamiento correcto en lo que a cambio de línea de backup respecta. En el caso de Paterna, las líneas de abastecimiento de comunicaciones son: fibra y radiofrecuencia.	06-Mayo/20-Septiembre
mp.si.1	Etiquetado	Se recomienda establecer una normativa que indique los pasos a seguir a la hora de etiquetar documentación, según lo establecido en el Esquema de Clasificación de la Información.	06-Mayo/20-Septiembre
mp.si.2	Criptografía	Se ha de establecer una política de criptografía que garantice confidencialidad e integridad de la información manejada en soportes de la información.	06-Mayo/20-Septiembre
mp.si.2	Criptografía	Se debe desarrollar y aplicar una política o normativa documentada que indique el uso de productos certificados componentes certificados). En caso contrario, debe estar aprobado por el responsable.	06-Mayo/20-Septiembre
mp.si.3	Custodia	Se debe actualizar la Norma de Seguridad Corporativa de forma que se haga referencia a las medidas a tener en cuenta en lo que a soportes de la información y su custodia se refiere	06-Mayo/20-Septiembre
mp.si.4	Transporte	Se ha de documentar un procedimiento que, en caso de entrega o salida de un soporte, se pueda verificar:	06-Mayo/20-

		- que registra cada salida y llegada de un soporte (tanto de aquellos electrónicos como no electrónicos -que hayan sido causa o consecuencia directa de la información electrónica dentro del alcance del ENS-) de las instalaciones de la organización. Dicho registro almacena tanto la etiqueta como el transportista encargado de su traslado. - que el uso de los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel.	Septiembre
mp.si.5	Borrado y destrucción	Se ha de documentar un procedimiento de eliminación y borrado de la información almacenada en los soportes que vayan a ser reutilizados	06-Mayo/20-Septiembre
mp.si.5	Borrado y destrucción	Se ha de incluir en el anterior procedimiento, la realización del borrado a través de medios o productos certificados	06-Mayo/20-Septiembre
mp.sw.1	Desarrollo de aplicaciones	N/A	
mp.sw.2	Aceptación y puesta en servicio	Se ha de procedimiento un documento que incluya la necesidad de realizar: - pruebas de aceptación en materia de seguridad. - pruebas para constatar que no se deteriora la seguridad de otros componentes del servicio. - que las pruebas se realizan en un entorno aislado (preproducción). - que las pruebas se realizan con datos ficticios o datos reales disociados o enmascarados, y en caso de que se realicen con datos reales se asegura el nivel de seguridad correspondiente	06-Mayo/20-Septiembre
mp.sw.2	Aceptación y puesta en servicio	Se debe aplicar un análisis de vulnerabilidades a las aplicaciones previo a su entrada en producción. En caso de detectar vulnerabilidad alguna, se han de establecer las medidas de seguridad pertinentes.	06-Mayo/20-Septiembre
mp.sw.2	Aceptación y puesta en servicio	En los casos en los que se pueda acceder al código fuente del software, se ha de realizar una auditoría, asegurando el desarrollo seguro durante el ciclo de vida de la aplicación.	06-Mayo/20-Septiembre

mp.info.1	Datos de carácter personal	No se requiere de mejoras o acciones al respecto	
mp.info.2	Calificación de la información	NewCo debe abordar la necesidad de definir un esquema de clasificación de la información y con ello, establecer las diferentes medidas de seguridad para cada nivel de sensibilidad de la información.	06-Mayo/20-Septiembre
mp.info.2	Calificación de la información	NewCo debe definir los procesos de etiquetado y calificación de la información, estableciendo: a) Su control de acceso. b) Su almacenamiento. c) La realización de copias. d) El etiquetado de soportes. e) Su transmisión telemática. f) Y cualquier otra actividad relacionada con dicha información.	06-Mayo/20-Septiembre
mp.info.3	Cifrado de la información	Se han de valorar e implantar las soluciones de cifrado de las que dispone Office365, a nivel de Correo y SharePoint. Se podría activar en conjunción con IRM/DLP de Office365. Se han de revisar que los protocolos y versiones usados son acordes a la guía 807 de Criptografía Se debe identificar si existe inventario de soportes de información y si contiene información confidencial, esta se debe cifrar.	06-Mayo/20-Septiembre
mp.info.4	Firma electrónica	Se ha de establecer un procedimiento de firma electrónica durante el proceso de comunicación, con el objetivo de preservar la confidencialidad de la información.	06-Mayo/20-Septiembre
mp.info.4	Firma electrónica	Se recomienda establecer el uso de firma electrónica a través del uso de elementos y productos certificados	06-Mayo/20-Septiembre
mp.info.4	Firma electrónica	N/A	
mp.info.5	Sellos de tiempo	N/A	
mp.info.6	Limpieza de documentos	Se ha de establecer un procedimiento de limpieza de metadatos.	06-Mayo/20-Septiembre
mp.info.9	Copias de seguridad (backup)	Junto con el Plan de Continuidad de Negocio, se han de establecer las necesidades de cada responsable a la hora de realizar copias de seguridad de la información, detallando,	06-Mayo/20-Septiembre

		frecuencia, sectores, bases de datos, etc. Se ha de incidir en la realización de pruebas de carga satisfactorias.	
mp.s.1	Protección del correo electrónico (e-mail)	Se precisa de una solución de cifrado de email o equivalente. Aunque actualmente las comunicaciones se cifran, se han de revisar que los protocolos y versiones usados son acordes a la guía 807 de Criptografía. Se ha de activar la protección básica gratuita disponible en Outlook 365. Se debe valorar la activación de Office ATP (Advanced Threat Protection) que proporciona Microsoft. Se han de revisar las referencias al uso de correo electrónico en las normas de uso de las herramientas de comunicaciones.	06-Mayo/20-Septiembre
mp.s.2	Protección de servicios y aplicaciones web	Se han de establecer las medidas necesarias en los sistemas que dispongan servicios publicados en la red, de forma que se impidan ataques que puedan afectar a la disponibilidad, integridad o confidencialidad de la información.	06-Mayo/20-Septiembre
mp.s.2	Protección de servicios y aplicaciones web	Para los servicios publicados en la red, se han de utilizar certificados cualificados	06-Mayo/20-Septiembre
mp.s.8	Protección frente a la denegación de servicio	Se propone la obtención de un sistema Anti-Ddos, adherido al cortafuegos. Además, se han de impedir el lanzamiento de ataques de Denegación de Servicio desde la propia organización.	06-Mayo/20-Septiembre
mp.s.8	Protección frente a la denegación de servicio	Se propone la obtención de un sistema Anti-Ddos, adherido al cortafuegos. Además, se han de impedir el lanzamiento de ataques de Denegación de Servicio desde la propia organización.	06-Mayo/20-Septiembre
mp.s.9	Medios Alternativos	Se ha de establecer una política o normativa documentada que establezca la obligatoriedad de aplicar las mismas garantías de seguridad a los medios alternativos que a los medios habituales.	06-Mayo/20-Septiembre

Anexo IV Análisis de Riesgos

Metodología de Análisis de Riesgos

La realización de la apreciación de riesgos que refleja este anexo se ha realizado según la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT v.3).
Esta metodología tiene como objeto ayudar a la organización a desarrollar un Análisis de Riesgos de la Seguridad de la Información y su posterior gestión.

Identificación de activos

Con el objetivo de identificar riesgos, el primer paso que se ha realizado es identificar y clasificar los activos que conforman los Sistemas de Información (en adelante SSII) que se circunscriben dentro del Alcance de NewCo. Estos SSII tratan y almacenan información considerada como relevante para la organización.
El siguiente esquema muestra los activos esenciales y de soporte que se han identificado:

- Activos esenciales
    - [SERV] Servicios prestados
        - [S_GRC] Consultoria
        - [S_NOC] Soporte al Usuario
        - [S_CIBER_SOC] SOC
    - [DAT] DATOS
        - [D_GRC] Datos de Proyectos de Consultoría
        - [D_NOC] SU - Arquitectura y Configuración de Cliente
        - [D_CIBER_SOC] Arquitectura y Configuración de Cliente
- Activos de soporte
    - [E] Equipamiento
        - [HW] Equipos
            - [HW_FW] Infraestructura firewall corporativa Fortinet
            - [HW_SWITCH] Switches
            - [HW_PC] PC de usuario
            - [HW_AP] Access point (Wireless)
            - [HW_RO] Routers
            - [HW_PHONE] Terminales móviles y teléfonos
            - [HW_CORP] Infraestructura hardware corporativa
            - [HW_BIO] Dispositivos de acceso biométrico
            - [HW_NAS] NAS Copias de Seguridad Local
        - [COM] Comunicaciones
            - [COM_TLF] Centralita Teléfonos
            - [COM_INV] Red de acceso a invitados
            - [COM_VPN] Servicio de VPN (hw y sw)
            - [SW_INT] Intranet corporativa
            - [COM_LANCORP] LAN Corporativa
            - [COM_TLFPERS] Líneas móviles personal
            - [COM_DAT_INT] Líneas comunicaciones datos e internet (fijo)
        - [AUX] Elementos auxiliares

        - [AUX_AIR] Aire acondicionado CPD
        - [AUX_SAI] SAI
        - [AUX_SUM] Suministro eléctrico
- [SW] Aplicaciones
    - [SW_NPS] Network Policy Server
    - [SW_Zabbix] Sistema Monitorización - Zabbix
    - [SW_BCK] Infraestructura de backup
    - [SW_GLPI] GLPI
    - [SW_O365] Office365
    - [SW_SHR] Sharepoint
    - [SW_OUT] Outlook
    - [SW_AD] Infraestructura de Active Directory
    - [SW_FS] Servidor de ficheros corporativos
    - [SW_QR] QRadar SIEM
    - [SW_Pass] Gestor de contraseñas
    - [SW_AntiV] AntiVirus
    - [SW_WS] Máquina Virtual Windows Server
- [SP] Servicios Internos
    - [SI_Correo] Servicio de Correo Electrónico
- [L] Instalaciones
    - [INST_VLC] Armario comunicaciones Valencia
    - [INST_CPDVAL] CPD Valencia
    - [INST_OFVLC] Oficinas Valencia
    - [INST_OFMAD] Oficinas Madrid
- [P] Personal
    - [PERS_TEC] Personal técnico
    - [PERS_GRC] Personal de consultoría
    - [PERS_SOC] Personal del Centro Operativo de Seguridad
    - [PERS_NOC] Personal del Centro de Operaciones y Soporte al Usuario
    - [PERS_PERS] Personas

El conjunto de activos identificados previamente debe asociarse a un propietario, el cual es responsable de la gestión del riesgo que se realice en la última fase (Plan de Tratamiento de Riesgos).
La matriz de asignación de activos se corresponde a la siguiente tabla:

Tipología de Activo	Propietario
Activos Esenciales [Información]	CEO
Activos esenciales [Servicios]	CEO
Equipamiento	CISO
Servicios Subcontratados	
Personal	Responsable de RRHH
Instalaciones	Responsable de Instalaciones

Dependencias de los activos

Los activos que se han identificado en la fase anterior tienen establecidas un conjunto de dependencias entre ellos, representado a través de una estructura en forma de árbol y distribuido por capas, de forma que se permite conocer la difusión del impacto en caso de materializarse una amenaza sobre un activo. De esta forma, la valoración de los activos que dan soporte a los activos esenciales se realiza por herencia, permitiendo así conocer el impacto sobre dichos elementos por la repercusión que ocasionaría sobre los servicios prestados y la información tratada.

Se muestra a continuación la primera capa de dependencias del servicio [S_GRC].

Activo
[D_GRC]
[HW_PC]
[HW_PHONE]
[COM_DAT_INT]
[SW_O365]
[SI_CORREO]
[PERS_GRC]

Valoración de los activos

En el presente análisis de riesgos, la valoración de los activos se fija sobre los activos esenciales, según los criterios establecidos en la guía 803 del CCN-CERT de Valoración de Sistemas, representada según los siguientes valores:

- [A] Alta
- [M] Media
- [B] Bajo
- [0] Si valorar

Dichos valores cuantifican los efectos que tendría sobre un activo la materialización de una amenaza, en el peor de los escenarios posibles, sin tener en cuenta las salvaguardas presentes respecto a las dimensiones de seguridad, a saber:

- [D] Disponibilidad
- [I] Integridad
- [C] Confidencialidad
- [A] Autenticidad
- [T] Trazabilidad

Los activos de soporte, es decir, aquellos que sustentan a los activos esenciales, acumulan los valores de estos a través de las dependencias configuradas en el punto anterior. Se muestra en la siguiente tabla los valores resultantes:

CAPA	ACTIVO	[D]	[I]	[C]	[A]	[T]
[B] Activos esenciales						
	[SERV] Servicios prestados					
	[S_GRC] Gobierno, Riesgo y Cumplimiento	[B]				
	[S_NOC] Soporte al Usuario	[A]				
	[S_CIBER_SOC] SOC	[A]				
	[DAT] DATOS					
	[D_GRC] Datos de Proyectos de Consultoría		[M]	[A]	[M]	[M]
	[D_NOC] SU - Arquitectura y Configuración de Cliente		[M]	[A]	[M]	[M]
	[D_CIBER_SOC] Arquitectura y Configuración de Cliente		[M]	[A]	[M]	[M]
[E] Equipamiento						
	[HW] Equipos					
	[HW_FW] Infraestructura firewall corporativa Fortinet	[A]	[A]	[A]	[M]	[A]
	[HW_SWITCH] Switches	[A]	[A]	[A]	[M]	[A]
	[HW_PC] PC de usuario	[A]	[M]	[A]	[M]	[M]
	[HW_AP] Access point (Wireless)	[A]	[A]	[A]	[M]	[A]
	[HW_RO] Routers	[A]	[A]	[A]	[M]	[A]
	[HW_PHONE] Terminales móviles y teléfonos	[A]	[M]	[A]	[M]	[M]
	[HW_CORP] Infraestructura hardware corporativa	[A]	[A]	[A]	[M]	[A]
	[HW_BIO] Dispositivos de acceso biométrico	[A]	[A]	[A]	[M]	[A]
	[HW_NAS] NAS Copias de Seguridad Local	[A]	[M]	[A]	[M]	[M]
	[COM] Comunicaciones					
	[COM_TLF] Centralita Telefonos	[M+]	[M]	[M-]	[B]	[B]
	[COM_INV] Red de acceso a invitados	[A]	[0]	[B]	[B]	[B]

CAPA	ACTIVO	[D]	[I]	[C]	[A]	[T]
	[COM_VPN] Servicio de VPN (hw y sw)	[A]	[B]	[M]	[M]	[M]
	[SW_INT] Intranet corporativa	[M]	[M]	[B]	[M]	[B]
	[COM_LANCORP] LAN Corporativa	[A]	[A]	[A]	[M]	[A]
	[COM_TLFPERS] Líneas móviles personal	[A]	[M+]	[A]	[M]	[M]
	[COM_DAT_INT] Líneas comunicaciones datos e internet (fijo)	[A]	[A]	[A-]	[M]	[M]
	[AUX] Elementos auxiliares					
	[AUX_AIR] Aire acondicionado CPD	[A]	[A]	[A]	[M]	[A]
	[AUX_SAI] SAI	[A]	[A]	[A]	[M]	[A]
	[AUX_SUM] Suministro eléctrico	[A]	[A]	[A]	[M]	[A]
	[SW] Aplicaciones					
	[SW_NPS] Network Policy Server	[A]	[A]	[A]	[M]	[A]
	[SW_Zabbix] Sistema Monitorización - Zabbix	[A]	[M]	[A]	[M]	[M]
	[SW_BCK] Infraestructura de backup	[A-]	[M]	[A]	[M]	[M]
	[SW_GLPI] GLPI	[A]	[A]	[A]	[M]	[A]
	[SW_O365] Office365	[A]	[M]	[A]	[M]	[M]
	[SW_SHR] Sharepoint	[A]	[M]	[A]	[M]	[M]
	[SW_OUT] Outlook	[A]	[M]	[A]	[M]	[M]
	[SW_AD] Infraestructura de Active Directory	[A]	[A]	[A]	[M]	[A]
	[SW_FS] Servidor de ficheros corporativos	[A]	[M]	[A]	[M]	[M]
	[SW_QR] QRadar SIEM	[A]	[M]	[A]	[M]	[M]
	[SW_Pass] Gestor de contraseñas	[M]	[M]	[A]	[M]	[M]
	[SW_AntiV] AntiVirus	[A]	[M]	[A]	[M]	[M]
	[SW_WS] Máquina Virtual Windows Server Paterna	[A]	[M]	[A]	[M]	[M]
[SI] Servicios internos						
	[SI_Correo] Servicio de Correo Electrónico	[A]	[M]	[A]	[M]	[M]
[L] Instalaciones						
	[INST_VLC] Armario comunicaciones Valencia	[A]	[A]	[A]	[M]	[A]
	[INST_CPDVAL] CPD Valencia	[A]	[A]	[A]	[M]	[A]
	[INST_OFVLC] Oficinas Valencia	[A]	[A]	[A]	[M]	[A]
	[INST_OFMAD] Oficinas Madrid	[A]	[A]	[A]	[M]	[A]
[P] Personal						
	[PERS_TEC] Personal técnico	[A]	[M]	[A]	[M]	[M]
	[PERS_GRC] Personal de consultoría	[M]	[M]	[A]	[M]	[M]
	[PERS_SOC] Personal del Centro Operativo de Seguridad	[A]	[M]	[A]	[M]	[M]
	[PERS_NOC] Personal del Centro de Operaciones y Soporte al Usuario	[A]	[M]	[A]	[M]	[M]
	[PERS_PERS] Personas	[A]	[A]	[A]	[M]	[A]

Amenazas

A continuación, se muestran las amenazas asociadas a cada uno de los activos materiales. Las amenazas impactan en los activos de distinta forma según la naturaleza de estos. Se detalla a continuación, las amenazas más frecuentes para los activos según su tipología y valorando, a través del impacto y la frecuencia, las consecuencias que tendría una materialización de la amenaza en las dimensiones de la seguridad.

CRITERIOS	PROBABILIDAD	IMPACTO (para cada dimensión)

0	Inexistente
MR	Muy raro
PP	Poco probable
P	Posible
MA	Muy alto
CS	Casi seguro

El activo no se degrada en absoluto — Degradación total del activo

0% … 50% … 100%

Activos de Soporte	Prob.	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento						
[HW] Equipos						
[HW_FW] Infraestructura firewall corporativa Fortinet		50%		50%		
[I.5] Avería de origen físico o lógico	MR	30%				
[I.6] Corte del suministro eléctrico	P	50%				
[E.2] Errores del administrador del sistema / de la seguridad	PP	30%		10%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	10%				
[A.23] Manipulación del hardware	PP	50%		50%		
[HW_SWITCH] Switches		50%		50%		
[I.5] Avería de origen físico o lógico	MR	30%				
[A.23] Manipulación del hardware	P	50%		50%		
[HW_PC] PC de usuario		70%	50%	50%		
[I.5] Avería de origen físico o lógico	P	50%				
[E.8] Difusión de software dañino	MR	50%	50%	50%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	PP	70%				
[A.11] Acceso no autorizado	PP		50%	50%	50%	50%
[A.23] Manipulación del hardware	PP	50%		50%		
[A.25] Robo de equipos	PP	50%		50%		
[HW_AP] Access point (Wireless)		50%		50%		
[I.5] Avería de origen físico o lógico	PP	10%				
[A.23] Manipulación del hardware	PP	50%		50%		
[HW_RO] Routers		50%		50%		
[I.5] Avería de origen físico o lógico	MR	30%				
[A.23] Manipulación del hardware	PP	50%		50%		
[HW_PHONE] Terminales móviles y teléfonos		70%	50%	70%		
[I.5] Avería de origen físico o lógico	MR	50%				
[I.8] Fallo de servicios de comunicaciones	MR	50%				
[E.8] Difusión de software dañino	P	70%	30%	50%		
[A.11] Acceso no autorizado	PP		50%	70%	50%	50%
[A.23] Manipulación del hardware	P	50%		50%		
[A.25] Robo de equipos	PP	10%		50%		
[HW_CORP] Infraestructura hardware corporativa		50%	30%	50%		
[I.5] Avería de origen físico o lógico	MR	30%				
[I.6] Corte del suministro eléctrico	MA	30%				
[E.2] Errores del administrador del sistema / de la seguridad	MR	30%	30%			
[E.8] Difusión de software dañino	P					
[A.23] Manipulación del hardware	PP	50%		50%		
[HW_BIO] Dispositivos de acceso biométrico		30%				
[I.5] Avería de origen físico o lógico	MR	30%				

Activos de Soporte	Prob.	[D]	[I]	[C]	[A]	[T]
[A.23] Manipulación del hardware	PP	30%				
[HW_NAS] NAS Copias de Seguridad Local		10%		0%		
[I.5] Avería de origen físico o lógico	P	10%		0%		
[A.23] Manipulación del hardware	P	10%		0%		
[COM] Comunicaciones						
[COM_TLF] Centralita Telefonos Alcatel		10%				
[I.8] Fallo de servicios de comunicaciones	PP	10%				
[COM_INV] Red de acceso a invitados				10%	10%	
[A.11] Acceso no autorizado	PP			10%	10%	10
[COM_VPN] Servicio de VPN (hw y sw)		30%				
[I.8] Fallo de servicios de comunicaciones	P	30%				
[SW_INT] Intranet corporativa		30%				
[E.2] Errores del administrador del sistema / de la seguridad	MR	30%				
[COM_LANCORP] LAN Corporativa		5%				
[E.2] Errores del administrador del sistema / de la seguridad	MR	5%				
[COM_TLFPERS] Líneas móviles personal		10%				
[I.8] Fallo de servicios de comunicaciones	MR	10%				
[COM_DAT_INT] Líneas comunicaciones datos e internet (fijo)		10%				
[I.8] Fallo de servicios de comunicaciones	MR	10%				
[AUX] Elementos auxiliares						
[AUX_AIR] Aire acondicionado CPD		30%				
[I.5] Avería de origen físico o lógico	MR	30%				
[AUX_SAI] SAI		50%				
[I.5] Avería de origen físico o lógico	MR	50%				
[AUX_SUM] Suministro electrico		90%				
[I.6] Corte del suministro eléctrico	P	90%				
[SW] Aplicaciones						
[SW_NPS] Network Policy Server		50%				
[E.2] Errores del administrador del sistema / de la seguridad	MR	50%				
[SW_Zabbix] Sistema Monitorización - Zabbix			40%		20%	20%
[E.3] Errores de monitorización (log)	P		100%		20%	20%
[SW_BCK] Infraestructura de backup			10%			
[E.4] Errores de configuración	P		10%			
[SW_GLPI] GLPI		5%	70%	50%		
[E.1] Errores de los usuarios	PP		70%			
[E.20] Vulnerabilidades de los programas (software)	P	1%	30%	50%		
[E.21] Errores de mantenimiento / actualización de programas (software)	PP	5%				
[A.11] Acceso no autorizado	PP		25%	30%		
[SW_O365] Office365		80%	50%	60%	80%	
[E.1] Errores de los usuarios	MR	25%	10%	40%		
[E.19] Fugas de información	PP			40%		
[A.5] Suplantación de la identidad	PP		50%	50%	80%	
[A.11] Acceso no autorizado	PP		50%	60%	50%	50%
[A.24] Denegación de servicio	PP	80%				
[SW_SHR] Sharepoint		50%	50%	60%		

Activos de Soporte	Prob.	[D]	[I]	[C]	[A]	[T]
[E.19] Fugas de información	PP			60%		
[E.20] Vulnerabilidades de los programas (software)	PP	50%	50%			
[A.11] Acceso no autorizado	P		30%	60%	50%	50%
[A.15] Modificación de la información	MR		30%			
[A.19] Revelación de información	MR			60%		
[A.24] Denegación de servicio	MR	50%				
[SW_OUT] Outlook		50%	30%	60%		
[E.19] Fugas de información	PP			60%		
[A.11] Acceso no autorizado	PP		30%	60%	50%	50%
[A.15] Modificación de la información	MR		30%			
[A.19] Revelación de información	MR			60%		
[A.24] Denegación de servicio	MR	50%				
[SW_AD] Infraestructura de Active Directory		10%				
[E.2] Errores del administrador del sistema / de la seguridad	PP	10%				
[E.20] Vulnerabilidades de los programas (software)	PP	10%				
[SW_FS] Servidor de ficheros corporativos			10%	50%		
[E.19] Fugas de información	PP			50%		
[A.11] Acceso no autorizado	PP		10%	50%	50%	50%
[SW_QR] QRadar SIEM		10%	20%	20%		
[E.2] Errores del administrador del sistema / de la seguridad	PP	10%	20%	20%		
[E.20] Vulnerabilidades de los programas (software)	P	10%	20%	20%		
[SW_Pass] Gestor de contraseñas		25%	50%	25%		
[E.1] Errores de los usuarios	MR	5%	50%	25%		
[E.2] Errores del administrador del sistema / de la seguridad	MR	25%	30%	10%		
[E.20] Vulnerabilidades de los programas (software)	P	25%	30%	20%		
[SW_AntiV] AntiVirus		35%	30%	20%		
[E.20] Vulnerabilidades de los programas (software)	P	35%	30%	20%		
[SW_SOC_MISP] Inteligencia de amenazas de código abierto		15%	30%	20%		
[E.20] Vulnerabilidades de los programas (software)	P	15%	30%	20%		
[SW_WS] Máquina Virtual Windows Server		50%	40%	25%		
[E.2] Errores del administrador del sistema / de la seguridad	PP	50%	40%	25%		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	25%	10%			
[SI] Servicios Internos						
[SI_Correo] Servicio de Correo Electrónico						
[L] Instalaciones						
[INST_VLC] Armario comunicaciones Valencia		50%	50%			
[I.1] Fuego	MR	50%	50%			
[I.2] Daños por agua	MR	50%	50%			
[INST_CPDVAL] CPD Valencia		70%	25%	25%		
[I.1] Fuego	MR	70%				
[I.2] Daños por agua	MR	70%				
[A.11] Acceso no autorizado	MR		25%	25%	50%	50%
[INST_OFVLC] Oficinas Valencia		50%				
[I.1] Fuego	MR	50%				
[I.2] Daños por agua	MR	50%				

Activos de Soporte	Prob.	[D]	[I]	[C]	[A]	[T]
[INST_OFMAD] Oficinas Madrid		50%				
[I.1] Fuego	MR	50%				
[I.2] Daños por agua	MR	50%				
[P] Personal						
[PERS_TEC] Personal técnico		25%		50%		
[E.19] Fugas de información	PP			50%		
[E.28] Indisponibilidad del personal	PP	25%				
[A.19] Revelación de información	PP			50%		
[PERS_GRC] Personal de Consultoria		30%		70%		
[E.19] Fugas de información	PP			70%		
[E.28] Indisponibilidad del personal	PP	30%				
[A.19] Revelación de información	PP			70%		
[PERS_SOC] Personal del Centro Operativo de Seguridad		60%		70%		
[E.19] Fugas de información	P			70%		
[E.28] Indisponibilidad del personal	PP	60%				
[A.19] Revelación de información	P			70%		
[PERS_COSU] Personal del Centro de Operaciones y Soporte al Usuario		70%		60%		
[E.19] Fugas de información	P			60%		
[E.28] Indisponibilidad del personal	MR	70%				
[A.19] Revelación de información	P			60%		
[PERS_PERS] Personas		50%		50%		
[E.19] Fugas de información	P			10%		
[E.28] Indisponibilidad del personal	MR	50%				
[A.19] Revelación de información	P			50%		

Salvaguardas

Una vez identificado el riesgo inherente, se ha analizado el estado de seguridad de la entidad, conociendo así el riesgo actual de la entidad. Se refleja a continuación el estado de la seguridad de NewCo, previo a la adecuación del Esquema Nacional de Seguridad, obtenido a través del análisis del estado de seguridad según los controles que son de aplicación para el SGSI, siendo estos el Anexo II del Esquema Nacional de Seguridad:

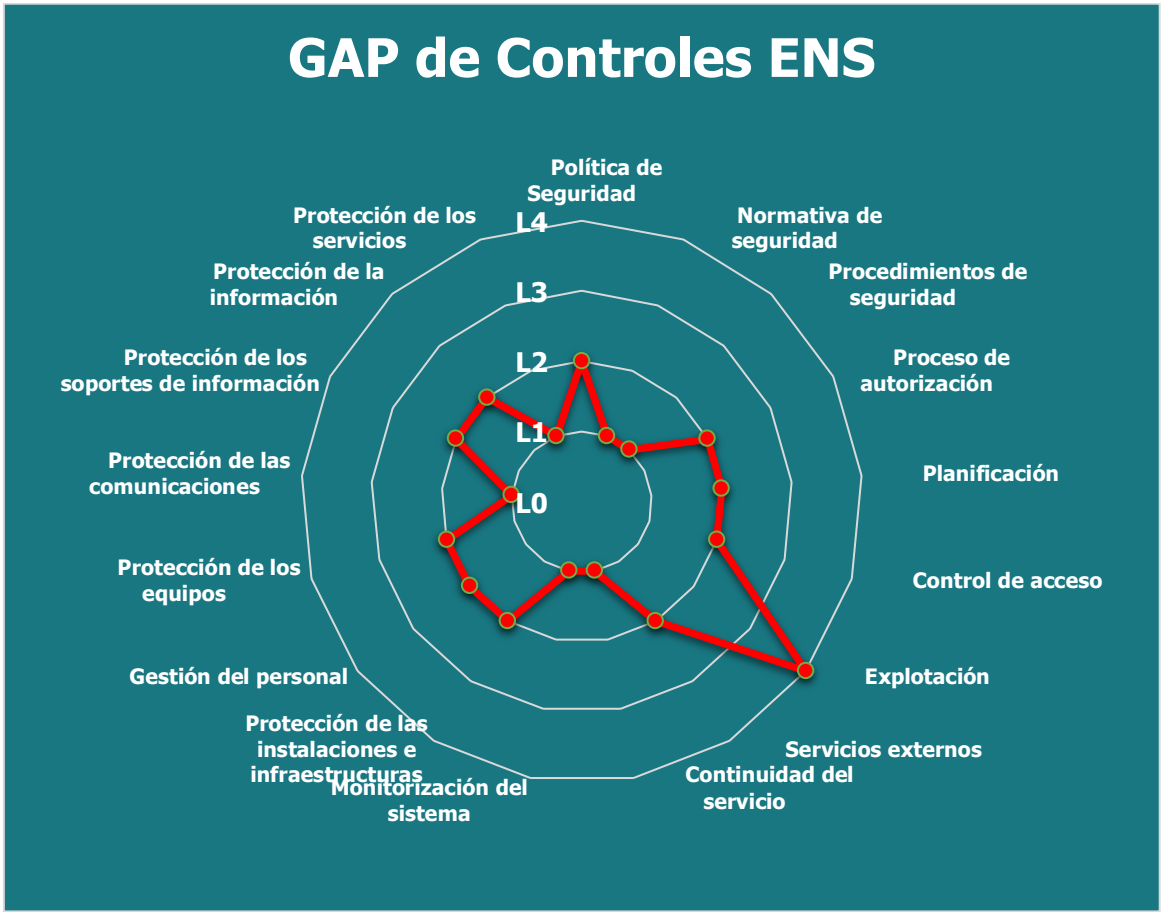


Ilustración 1: Controles de seguridad según Esquema Nacional de Seguridad

Riesgo actual

Se muestra a continuación los principales riesgos detectados. Para una mejor visualización, aquellos riesgos que superan el umbral de aceptación (el cual se ha determinado en un valor de "2,6" por la Alta Dirección) se muestran en tonalidad naranja.

Activo	Amenaza	DICAT	Riesgo actual
[HW_PHONE] Terminales móviles y teléfonos	[I.5] Avería de origen físico o lógico	[D]	{4,2}
[INST_OFVAL] Oficinas Valencia	[I.2] Daños por agua	[D]	{3,8}
[SW_Zabbix] Sistema Monitorización - Zabbix	[E.3] Errores de monitorización (log)	[I]	{3,8}
[HW_PC] PC de usuario	[I.5] Avería de origen físico o lógico	[D]	{3,8}
[SW_Pass] Gestor de contraseñas	[E.1] Errores de los usuarios	[C]	{3,7}
[SW_Pass] Gestor de contraseñas	[E.2] Errores del administrador del sistema / de la seguridad	[C]	{3,7}
[COM_CITRIX] CITRIX	[A.11] Acceso no autorizado	[C]	{3,3}
[COM_CITRIX] CITRIX	[A.11] Acceso no autorizado	[A]	{3,3}
[HW_PHONE] Terminales móviles y teléfonos	[A.11] Acceso no autorizado	[C]	{3,3}
[SW_Pass] Gestor de contraseñas	[E.20] Vulnerabilidades de los programas (software)	[C]	{3,3}
[HW_PHONE] Terminales móviles y teléfonos	[I.8] Fallo de servicios de comunicaciones	[D]	{3,3}
[HW_PHONE] Terminales móviles y teléfonos	[E.8] Difusión de software dañino	[D]	{3,2}
[SW_SHR] Sharepoint	[A.11] Acceso no autorizado	[C]	{3,2}
[HW_VIRT] Infraestructura hardware corporativa	[I.6] Corte del suministro eléctrico	[D]	{3,1}
[SW_GLPI] GLPI	[E.20] Vulnerabilidades de los programas (software)	[C]	{3,1}
[PERS_SOC] Personal del Centro Operativo de Seguridad	[E.19] Fugas de información	[C]	{3,0}
[HW_PC] PC de usuario	[A.11] Acceso no autorizado	[C]	{3,0}
[HW_PHONE] Terminales móviles y teléfonos	[A.11] Acceso no autorizado	[I]	{3,0}
[HW_PC] PC de usuario	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	{2,9}
[HW_PHONE] Terminales móviles y teléfonos	[E.8] Difusión de software dañino	[C]	{2,9}
[HW_PC] PC de usuario	[A.25] Robo de equipos	[C]	{2,9}
[HW_PHONE] Terminales móviles y teléfonos	[A.25] Robo de equipos	[C]	{2,9}
[HW_PC] PC de usuario	[A.25] Robo de equipos	[D]	{2,9}
[COM_VPN] Servicio de VPN (hw y sw)	[I.8] Fallo de servicios de comunicaciones	[D]	{2,9}
[SW_WS] Máquina Virtual Windows Server	[E.21] Errores de mantenimiento / actualización de programas (software)	[D]	{2,8}
[PERS_SOC] Personal del Centro Operativo de Seguridad	[A.19] Revelación de información	[C]	{2,8}

[HW_PC] PC de usuario	[A.23] Manipulación del hardware	[D]	{2,8}
[HW_PC] PC de usuario	[A.23] Manipulación del hardware	[C]	{2,7}
[SW_AntiV] AntiVirus Sophos	[E.20] Vulnerabilidades de los programas (software)	[I]	{2,7}
[PERS_PERS] Personas	[A.19] Revelación de información	[C]	{2,6}
[SW_WS] Máquina Virtual Windows Server	[E.21] Errores de mantenimiento / actualización de programas (software)	[I]	{2,6}
[AUX_SUM] Suministro eléctrico	[I.6] Corte del suministro eléctrico	[D]	{2,5}
[HW_PHONE] Terminales móviles y teléfonos	[A.23] Manipulación del hardware	[C]	{2,5}
[HW_PHONE] Terminales móviles y teléfonos	[A.23] Manipulación del hardware	[D]	{2,5}
[HW_PC] PC de usuario	[E.8] Difusión de software dañino	[C]	{2,5}
[HW_PC] PC de usuario	[E.8] Difusión de software dañino	[D]	{2,5}
[HW_PHONE] Terminales móviles y teléfonos	[E.8] Difusión de software dañino	[I]	{2,5}
[SW_OUT] Outlook	[E.19] Fugas de información	[C]	{2,5}
[SW_SHR] Sharepoint	[E.19] Fugas de información	[C]	{2,5}
[SW_GLPI] GLPI	[E.20] Vulnerabilidades de los programas (software)	[I]	{2,4}
[SW_AntiV] AntiVirus Sophos	[E.20] Vulnerabilidades de los programas (software)	[D]	{2,4}
[SW_QR] QRadar SIEM	[E.20] Vulnerabilidades de los programas (software)	[C]	{2,4}
[SW_AntiV] AntiVirus Sophos	[E.20] Vulnerabilidades de los programas (software)	[C]	{2,4}
[SW_OUT] Outlook	[A.11] Acceso no autorizado	[C]	{2,3}
[SW_GLPI] GLPI	[E.1] Errores de los usuarios	[I]	{2,3}
[SW_WS] Máquina Virtual Windows Server	[E.2] Errores del administrador del sistema / de la seguridad	[I]	{2,2}
[PERS_GRC] Personal de consultoria	[E.19] Fugas de información	[C]	{2,1}
[SW_Pass] Gestor de contraseñas	[E.20] Vulnerabilidades de los programas (software)	[D]	{2,1}
[HW_NAS] NAS Copias de Seguridad Local	[I.5] Avería de origen físico o lógico	[D]	{2,1}
[PERS_SOC] Personal del Centro Operativo de Seguridad	[E.28] Indisponibilidad del personal	[D]	{2,0}
[HW_RO] Routers	[A.23] Manipulación del hardware	[D]	{1,9}
[HW_AP] Access point (Wireless)	[A.23] Manipulación del hardware	[D]	{1,9}
[HW_RO] Routers	[A.23] Manipulación del hardware	[C]	{1,8}
[HW_VIRT] Infraestructura hardware corporativa	[A.23] Manipulación del hardware	[C]	{1,8}
[HW_AP] Access point (Wireless)	[A.23] Manipulación del hardware	[C]	{1,8}

[SW_SHR] Sharepoint	[E.20] Vulnerabilidades de los programas (software)	[D]	{1,8}
[SW_WS] Máquina Virtual Windows Server	[E.2] Errores del administrador del sistema / de la seguridad	[C]	{1,8}
[HW_PHONE] Terminales móviles y teléfonos	[A.25] Robo de equipos	[D]	{1,7}
[HW_NAS] NAS Copias de Seguridad Local	[A.23] Manipulación del hardware	[D]	{1,7}
[SW_WS] Máquina Virtual Windows Server	[E.2] Errores del administrador del sistema / de la seguridad	[D]	{1,6}
[SW_QR] QRadar SIEM	[E.2] Errores del administrador del sistema / de la seguridad	[C]	{1,6}
[PERS_PERS] Personas	[E.19] Fugas de información	[C]	{1,5}
[SW_GLPI] GLPI	[A.11] Acceso no autorizado	[C]	{1,5}
[SW_Pass] Gestor de contraseñas	[E.20] Vulnerabilidades de los programas (software)	[I]	{1,5}
[SW_SHR] Sharepoint	[A.19] Revelación de información	[C]	{1,5}
[SW_OUT] Outlook	[A.19] Revelación de información	[C]	{1,5}
[SW_QR] QRadar SIEM	[E.20] Vulnerabilidades de los programas (software)	[D]	{1,4}
[SW_Pass] Gestor de contraseñas	[E.1] Errores de los usuarios	[I]	{1,4}
[PERS_TEC] Personal técnico	[E.28] Indisponibilidad del personal	[D]	{1,3}
[SW_Pass] Gestor de contraseñas	[E.2] Errores del administrador del sistema / de la seguridad	[I]	{1,1}

Resumen y contextualización de los riesgos

A raíz de estos resultados, el resumen de los riesgos más significativos se corresponde a los siguientes hechos:

Resumen de riesgos
Existe una falta de control sobre la gestión de las credenciales de acceso a sistemas internos y de clientes, no existiendo unas directrices formales para su custodia y mantenimiento.
Se ha informado de la existencia de humedades y pequeñas fugas de agua ocurridas en el pasado en la zona del CPD y del almacén. Aunque las goteras del CPD han sido solventadas, el riesgo existente en el almacén sigue existiendo debido a la ubicación de una canaleta.
A través del análisis de la entidad, existe una importante dependencia tecnológica de proveedores en el Cloud, como por ejemplo Azure o Vodafone, para el correcto funcionamiento del servicio.
Respecto al inventario de activos, se detecta que no existe un repositorio único donde se almacenen correctamente y de forma actualizada, los activos de la entidad.
Se detecta un riesgo asociado a la salida por internet, ya que algunos servicios salen por la red de Jazztel, la cual no dispone de las mismas medidas de seguridad que la salida de red de Vodafone. Sólo dispone de un cortafuegos.

Los equipos de usuario, que por la operativa diaria almacenan información determinada como confidencial o secreta, no disponen de cifrado de disco.
Las destructoras de papel de las que dispone la entidad no cumplen con el nivel 5 de la norma DIN 66399 para la destrucción de información clasificada, tal y como se requiere por parte del Centro Nacional de Inteligencia. Este riesgo aplica al departamento de Gobierno de Seguridad de la Información.
Se ha informado que para diversos accesos a los sistemas de información se habilitan instancias de identificación independientes en lugar de un inicio de sesión unificado (SSO).
Se ha detectado que el sistema operativo que soporta el firewall físico de Valencia está obsoleto (siendo su última versión de 2015), aunque la versión de firmas está actualizada.
Además, se detecta un riesgo de incumplimiento legal en la operativa de migración de buzones en la baja de un empleado, ya que en ocasiones se accede al repositorio de e-mails, con la posibilidad de ver correos nuevos.
Se detecta un riesgo en la aplicación de monitorización Zabbix, ya que se encuentra integrado con la interfaz de Mercadona. Además, como aplicación de alta importancia para la monitorización de clientes, se identifica un riesgo sobre la disponibilidad del servicio.

Además del resumen de riesgos detallado en el punto anterior, existe un conjunto de riesgos asociados al contexto de la organización. Se explican a continuación los principales riesgos identificados por el equipo consultor:

ID	Riesgos de contexto
[RC1]	En el contexto y entorno en el cual NewCo realiza sus actividades, existe una gran dependencia de un cliente, el cual requiere una demanda de recursos notable. Este hecho implica como consecuencia una alta volatilidad respecto a la gestión de capacidades o en la rotación de personal, que pueden desencadenar en un riesgo en la prestación de servicios.
[RC2]	En los últimos tiempos se han producido diversos cambios en la legislación que elevan el riesgo de incumplimiento en el caso de que no se apliquen en la entidad.
[RC3]	La estructura de la organización ha llevado a cabo en los últimos dos años un crecimiento sustancial en lo que a personal se refiere, llegando a duplicar las cifras de plantilla en este tramo de tiempo. Dicho aumento de la plantilla ha inferido en necesidades, como, por ejemplo: • El establecimiento de ubicaciones físicas alternativas, • la determinación de Planes de Emergencia, • y la adecuación de su parque tecnológico, • entre otros. Este hecho podría implicar situaciones en las que se desconociera de forma fehaciente la manera de actuar por parte de las Personas de NewCo.

PLAN TRATAMIENTO DE RIESGOS

La propuesta para el tratamiento de riesgos identificados en el presente documento se ha desarrollado en el documento independiente Plan de Tratamiento de Riesgos, en el cual viene recogido el detalle de las medidas y salvaguarda

BIBLIOGRAFIA

Para la elaboración del presente documento se han tomado como referencia los siguientes documentos/enlaces:

- GUÍA DE SEGURIDAD (CCN-STIC-800) ESQUEMA NACIONAL DE SEGURIDAD GLOSARIO DE TÉRMINOS Y ABREVIATURAS;
- Guía de Seguridad de las TIC CCN-STIC 801 ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES;
- Guía de Seguridad de las TIC CCN-STIC 825 ESQUEMA NACIONAL DE SEGURIDAD CERTIFICACIONES 27001 Noviembre 2013;
- Esquema Nacional de Seguridad RD 3/2010, de 8 de enero;
- Guía de Seguridad de las TIC CCN-STIC 809 Declaración, certificación y probación provisional de conformidad con el ENS y distintivos de cumplimiento;
- Perfil de Cumplimiento Específico CCN-STIC 886 Perfil de Cumplimiento Específico para Sistemas Cloud Privados y Comunitarios;
- GUÍA ESTRATÉGICA EN SEGURIDAD PARA ENTIDADES LOCALES (FEMP TOMO I);
- GUÍA ESTRATÉGICA EN SEGURIDAD PARA ENTIDADES LOCALES (FEMP TOMO II);
- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html;
- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html;
- http://www.avantic.net/uploads/media/ENS03_CATEGORIZACION-SI-ENS_2011.pdf;
- https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html;
- https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html