PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA ADECUACIÓN FINAL E IMPLANTACIÓN DE LA PRIMERA OLEADA DEL PLAN DIRECTOR DE CIBERSEGURIDAD DE CETURSA SIERRA NEVADA Y SUS EMPRESAS ASOCIADAS

CE181960059/23

CETURSA SIERRA NEVADA S.A.
Plaza de Andalucía, 4 Edificio Cetursa
18196 Sierra Nevada, Monachil GRANADA
cetursa.es Tlf. +34 958 249100 - sierranevada@cetursa.es

Contenido

1.- ANTECEDENTES

Cetursa Sierra Nevada S.A. (Cetursa) es la empresa pública encargada de la gestión de la Estación de Esquí de Sierra Nevada.

Las características de la actividad de Cetursa hacen necesaria una fuerte implicación hacia la ciberseguridad. Recientemente, ha elaborado y presentado el Plan Estratégico de Seguridad, dividido en tres oleadas de Seguridad. La primera de ellas está compuesta por un total de 11 de iniciativas, las cuales son objeto del presente pliego.

Actualmente, la Dirección canalizará las acciones del Plan director de Seguridad llevadas a cabo por la empresa.

2.- OBJETO

El objeto de esta licitación es la contratación de los trabajos y servicios necesarios para LA adecuación final e implantación de la primera oleada del plan director de ciberseguridad de Cetursa Sierra Nevada y sus empresas asociadas.

Esta contratación pretende asegurar la adopción de las medidas técnicas, organizativas y normativas necesarias, en el ámbito de la seguridad de la información y de la ciberseguridad, con el objetivo de minimizar los riesgos de seguridad y asegurar el cumplimiento de las normativas en este ámbito.

3.- ALCANCE DE LOS TRABAJOS A REALIZAR

En este apartado se describe el alcance de los trabajos a desarrollar para cumplir con el objeto indicado en el contrato.

Partiendo del Plan Director de Seguridad realizado, se deben desarrollar las acciones descritas en cada una de las iniciativas de la Oleada 1 las cuales se describen a continuación:

3.1.- Fase de Gobierno.

3.1.1- Definición y formalización del Cuerpo Normativo de Seguridad

Realizar el desarrollo de un Marco y Cuerpo Normativo de Seguridad que tenga en cuenta las nuevas normativas y buenas prácticas en esta materia. Dicho alcance se desarrollará como un mecanismo de protección, pero también como un elemento base para la continuidad de negocio.

Dentro del alcance de este proyecto, se deben desarrollar documentos los cuales están comprendidos principalmente en las siguientes áreas o dominios de seguridad:

- Ciberseguridad ligada al personal
- Gestión de activos
- Clasificación, tratamiento y regulación del intercambio de la información
- Control de acceso a los sistemas
- Cifrado de la información y las comunicaciones
- Seguridad física de los sistemas y del entorno
- Seguridad ligada al mantenimiento y administración
- Protección y gestión del software
- Protección y gestión de redes
- Seguridad en el ciclo de vida de los sistemas
- Gestión de incidentes de ciberseguridad
- Ciberseguridad en la relación con terceros
- Gestión de la continuidad de negocio
- Auditoria de ciberseguridad

Para el desarrollo de los documentos se toma como referencia estándares internacionales y guías específicas de seguridad.

Como parte de la elaboración del Cuerpo Normativo de Seguridad, se deben realizar acciones continuas de soporte para ir generando cultura en la aplicación del cuerpo normativo, realizando actividades tales como:

- Involucración de stakeholders en la definición del alcance del Cuerpo Normativo de Seguridad
- Validación de los documentos del Cuerpo Normativo de Seguridad por parte de todas las áreas de la Organización
- Difusión del Cuerpo Normativo de Seguridad a todos los empleados de la Organización, mediante concienciación y formación

3.1.2.- Diseño del Plan de Adecuación al Esquema Nacional de Seguridad (ENS)

Realizar el diseño de un plan de acción para la adecuación y certificación de los sistemas de Cetursa en el Esquema Nacional de Seguridad, el cual contenga al menos, las siguientes fases:

- Análisis y categorización de sistemas de información
- Selección de medidas de seguridad aplicables
- Evaluación del nivel de adecuación del sistema de información
- Plan de acción para el cumplimiento

- Apoyo auditoría interna
- Acompañamiento en la certificación

3.1.3.- Establecimiento de un órgano de gobierno de seguridad (TOM)

Realizar el análisis del actual modelo operativo y de gobierno de Seguridad de la Información de la compañía, para posteriormente diseñar un modelo operativo aspiracional, para el cual a continuación, se enumeran las fases y principales tareas a desarrollar:

Fase I: Análisis de situación

- Entendimiento de los objetivos de seguridad, negocio y su estrategia
- Identificación del modelo de relación actual
- Análisis del Modelo de Gobierno y Operativo actual

Fase II: Evaluación del modelo

- Evaluación del Modelo actual
- Workshop comparativo entre varios modelos
- Definición aspiracional del Modelo Operativo

En esta fase se deberá evaluar, en base a toda la información analizada en el modelo anterior, cuál debe ser el modelo operativo futuro para cubrir las necesidades y los GAP identificados.

Fase III: Diseño del Modelo

- Diseño en detalle del Modelo Operativo
- Plan de acción a través de un modelo de transición

3.1.4.- Implementación de un plan de formación y concienciación avanzada

Diseñar un plan de formación y concienciación dirigido a mitigar el componente humano del ciber riesgo, el cual contenga al menos las siguientes tareas a desarrollar:

- Desarrollo del Plan de Formación y Concienciación
- Talleres de seguridad y de comunicación
- Campañas simuladas de ingeniería social (phishing, vishing y SMiShing).
- Píldoras formativas y/o Infografías
- Workshops

3.2.- Fase de protección

3.2.1.- Definición de un Programa de Seguridad Física

Evaluar la seguridad física de las instalaciones, identificando las vulnerabilidades de protección encontradas y abordando un estudio exhaustivo de la situación actual de la seguridad física en cada una de las instalaciones de la compañía, a fin de identificar las mejoras o correcciones necesarias.

Este plan deberá contener al menos las siguientes tareas:

- Conocimiento del entorno de las instalaciones
- Estudio de vulnerabilidades y del nivel de madurez actual.
- Evaluar el nivel de riesgos actual de la instalación (desde la perspectiva de seguridad física)
- Definir el nivel de madurez objetivo y las iniciativas para conseguirlo, así como una priorización de calendario y un plan de proyectos.

3.2.2.- Gestión e inventariado de activos

Definir un inventario centralizado de activos, que especifique dónde se encuentran y la posibilidad de controlar los accesos sobre ellos, además de incluir atributos como la criticidad, la sensibilidad de los datos y demás información de interés para la seguridad.

Este plan deberá contener al menos las siguientes tareas:

- Recopilar la información relativa a la gestión de activos desde un enfoque normativo, regulatorio y tecnológico.
- Definir los procedimientos y procesos que gobernarán la gestión de activos
- Identificar los activos HW y SW que componen los entornos o áreas dentro del alcance, así como a los propietarios y/o responsables de los mismos.
- Recopilar la información específica sobre los activos dentro del alcance (tipo, función, ubicación, criticidad, dependencias, etc.).

3.2.3.- Definición de un esquema de clasificación de datos

Realizar la identificación de todos los activos de información sensible, estableciendo un sistema de clasificación acorde a las necesidades planteadas por la compañía y que ayude a determinar las medidas de seguridad necesarias para salvaguardar su confidencialidad, integridad y disponibilidad.

Este plan deberá contener al menos las siguientes tareas:

- Crear un inventario de activos de información sensible y activos identificados.
- Dar soporte al etiquetado de los activos en base a una nomenclatura de identificación que facilite su localización.
- Realizar un análisis de riesgos de divulgación o acceso no autorizado de información.

3.2.4.- Implantación de un programa de gestión de terceros

Desarrollar un modelo de gestión segura de proveedores, que permita controlar adecuadamente los riesgos de seguridad asociados a los servicios externalizados.

Este plan deberá contener al menos las siguientes tareas:

- Analizar la situación actual
- Establecer el modelo de gobierno (roles y responsabilidades)
- Definir el modelo operativo de terceras partes, incluyendo entre otros procesos, modelo de controles, cuestionarios, categorización de peticiones, etc.
- Establecer KPIs y mecanismos de reporting
- Revisar propuesta de mejoras sobre el clausulado legal
- Establecer el flujo de relación con compras

3.3.- Fase de vigilancia

3.3.1.- Programa de gestión de vulnerabilidades

Diseñar y ejecutar un programa de gestión de vulnerabilidades que establezca de manera periódica la ejecución de escaneos de vulnerabilidad sobre los activos y sistemas de la compañía.

Este programa deberá contener al menos las siguientes tareas:

- Propuesta y validación del diseño de arquitectura
- Instalación y configuración de herramientas
- PoC: Primera política y escaneo
- Realizar escaneos de red para los sistemas no identificados
- Definir y ajustar políticas y escaneos
- Programar y lanzar escaneos

Para la ejecución de los escaneos de vulnerabilidades se deberán realizar escaneos automáticos, revisiones manuales y la elaboración del correspondiente plan de acción.

3.3.2.- Plan de pruebas periódicas de penetración

Realizar la definición y ejecución de un modelo de pentesting periódico.

Este modelo deberá contener al menos las siguientes tareas:

- Definición de objetivos y alcance
- Validación de escenarios y verificación de requerimientos
- Análisis y explotación de vulnerabilidades
- Identificación de contramedidas
- Realización de informes ejecutivos y técnicos

3.4.- Fase de resiliencia

3.4.1.- Implementación de un Proceso de gestión de Incidentes y un Sistema de Comunicación y gestión de Crisis

Diseñar un procedimiento de respuesta ante incidentes de seguridad que incluya los procesos de recuperación de los sistemas de información en caso de desastre o la contención o seguimiento de una posible brecha de información.

Además, se deberá definir un Sistema de Comunicación y gestión de Crisis que formalice el proceso de comunicación en situación de crisis.

Este modelo deberá contener al menos las siguientes tareas:

4.- ENTREGABLES Y CALENDARIO

Propuesta de desarrollo de las diferentes iniciativas la adecuación final e implantación de la primera oleada del plan director de ciberseguridad de Cetursa Sierra Nevada y sus empresas asociadas.

Plazo máximo de ejecución de los trabajos, 12 meses.

Luis Fernando Moreno Martínez David Cucharero López

VIDsigner code: 3B673607C6524DB882...

Luis Fernando Moreno Martínez

ANEXO I – REQUISITOS BOJA

ORGANIZACIÓN DE LA SEGURIDAD TIC Y LA PROTECCIÓN DE DATOS

EST. 1.2

«Artículo 5. Estructura organizativa de la Consejería en materia de seguridad de la información y seguridad interior.

1. La estructura organizativa de la seguridad de la información de la Consejería, de acuerdo con el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, regulado por el Real Decreto 3/2010, de 8 de enero, y del Decreto 1/2011, de 11 de enero, está compuesta por:

a) Comité de Seguridad Interior y Seguridad TIC.
b) Unidad de Seguridad TIC, cuya persona titular tendrá la condición de Responsable de Seguridad.
c) Responsables de la Información.
d) Responsables del Servicio.
e) Responsables del Sistema.

Además, en el ámbito de la Consejería, y de acuerdo con lo establecido en la normativa sobre protección de datos personales, deberán contemplarse las siguientes figuras:

a) El Delegado o Delegada de Protección de Datos.
b) Responsables del Tratamiento.
c) Encargados del Tratamiento.

Cada una de las entidades vinculadas o dependientes deberá disponer de una estructura organizativa de la seguridad de la información similar a la que se describe para la Consejería, con la salvedad de que no es necesaria la Unidad de Seguridad TIC, pero sí la figura de Responsable de Seguridad.

2. De acuerdo con el Decreto 171/2020, de 13 de octubre, la organización para la gestión de la seguridad interior se configura en la Consejería mediante la siguiente estructura:

a) Comité de Seguridad Interior y Seguridad TIC.
b) Unidad de Seguridad Interior.
c) Puntos Coordinadores de Seguridad.

De conformidad con lo previsto en el artículo 10.1 del Decreto 171/2020, de 13 de octubre, las entidades vinculadas o dependientes, además de su correspondiente Comité de Seguridad Interior y Seguridad TIC, podrán contar con una Unidad de Seguridad Interior cuando así lo consideren necesario en virtud del volumen o singularidad de sus activos. Su designación corresponderá al Comité de Seguridad Interior y Seguridad TIC de la entidad.»

OBLIGACIÓN DE CONOCER Y CUMPLIR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y LAS NORMAS DE SEGURIDAD DERIVADAS.

EST. 1.2

El artículo 10.1 de dicho decreto determina que cada Consejería y entidad deberá contar con un Comité de Seguridad TIC, que no tendrá carácter colegiado y que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada.

Cuatro. Se modifica el artículo 3, que queda redactado en los siguientes términos: «Artículo 3. Definiciones, objetivos y principios. 1. En lo referente a la política de seguridad de la información, serán aplicables las definiciones, objetivos y principios establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero. 2. Las definiciones, objetivos y principios básicos de la política de la seguridad interior son los dispuestos en los artículos 3, 4 y 5 del Decreto 171/2020, de 13 de octubre.»

Cinco. Se modifica el apartado 2 del artículo 4, que pasa a tener la siguiente redacción:
«2. Todas las personas empleadas que presten servicios en la Consejería o en sus entidades vinculadas o dependientes tienen la obligación de conocer y cumplir la política de seguridad de la información y las normas de seguridad derivadas, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC establecer mecanismos adecuados para que la información llegue a las personas afectadas.»

11. En el ámbito de la Seguridad Interior, el Comité de Seguridad Interior y Seguridad TIC tendrá asignadas las siguientes funciones:

a) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior de la Consejería.
b) Velar por la disponibilidad de los recursos necesarios para el desarrollo de las iniciativas y planes estratégicos definidos.
c) Establecer directrices comunes y supervisar el cumplimiento de la normativa de seguridad interior en el ámbito de la Consejería.
d) Designar a los miembros de la Unidad de Seguridad Interior, así como designar a su responsable.
e) Aprobar el modelo de relación con los Puntos Coordinadores de Seguridad Interior y tomar conocimiento de la designación de sus titulares.
f) Promover programas de formación, entrenamiento y concienciación sobre las medidas relativas a la seguridad interior entre el personal de la Consejería.
g) Analizar y adoptar decisiones para la prevención o para la respuesta a incidentes susceptibles de generar una crisis de seguridad en la Consejería.
h) Cualquier otra que se le asigne en materia de seguridad interior.

12. El Comité aprobará, por mayoría simple de sus miembros, sus propias reglas de organización, funcionamiento y adopción de acuerdos. La Unidad de Seguridad TIC podrá ejercer como Responsable de Seguridad de las entidades vinculadas o dependientes de la Consejería, si es nombrada como tal por el Comité de Seguridad Interior y Seguridad TIC de las mismas, previo informe favorable del órgano directivo del que dependa jerárquicamente dicha Unidad.»

COOPERACIÓN CON OTROS ÓRGANOS Y ADMINISTRACIONES EN MATERIA DE SEGURIDAD TIC Y PROTECCIÓN DE DATOS PERSONALES

RES. 1.2

«Artículo 22. Cooperación en materia de seguridad TIC.

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la seguridad de la información, se fomentará, en coordinación con la Unidad de Seguridad TIC Corporativa para los agentes externos a la Junta de Andalucía, el establecimiento de mecanismos de coordinación con al menos los siguientes agentes:

a) La Agencia Digital de Andalucía.

b) El Comité de Seguridad Interior y Seguridad TIC de la Junta de Andalucía.

c) La Unidad de Seguridad TIC de la Junta de Andalucía.

d) AndalucíaCERT (centro especializado y orientado a la prevención, detección y

respuesta a incidentes y amenazas de seguridad).

e) El Consejo de Transparencia y Protección de Datos de Andalucía.

f) CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.

g) La Agencia Española de Protección de Datos (AEPD).

h) El Instituto Nacional de Ciberseguridad (INCIBE).

i) El Departamento contra el cibercrimen de la Guardia Civil y Brigada Central de Investigación Tecnológica del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

Adicionalmente, se podrán mantener contactos con otros organismos y entidades, incluyendo los entes instrumentales de la Consejería.

ANEXO II – PLAN DE ACCIÓN DE OLEADA 1