Política Global de Seguridad  
HuescaTelecom



Departamento de Seguridad HuescaTelecom  
2023

* **Introducción**

Actualmente la información se ha convertido en uno de los activos más importantes para cualquier organización, independientemente de su actividad. Por eso se buscará, en el presente documento, desarrollar un conjunto de proyectos con el objetivo de reducir los riesgos a los que está sometida la organización.

Esta política define los principios generales de la organización en relación a la seguridad, con el objetivo de garantizar la seguridad tanto de los empleados de la organización como de los clientes.

Se priorizará la seguridad de la información, ya que es la parte fundamental de la organización. Está política será revisada y/o actualizada anualmente por los responsables de seguridad, que deberán realizar una evaluación continua de la misma con el objetivo de detectar errores o fallos de seguridad, con el previo permiso del equipo directivo. Estos cambios serán comunicados a todos los empleados de la organización

* **Tabla de revisión**

| **Fecha** | **Revisado por:** | **Aprobado por:** | **Versión** | **Vigente hasta:** | **Notas** | **Comunicado** |
| --- | --- | --- | --- | --- | --- | --- |
| 12/1/2023 | Departamento Seguridad HuescaTelecom | Director General HuescaTelecom | 1.0 | 12/1/2024 |  | ✅ |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* **Principios de seguridad**

La seguridad de la organización está basada en los siguientes principios:

* + **Principio de confidencialidad:** la organización garantizará la confidencialidad de la información de sus clientes mediante la implantación de medidas de seguridad.
  + **Principio de disponibilidad:** la organización garantizará que los recursos requeridos por los clientes estén totalmente disponibles cuando el usuario lo requiera.
  + **Principio de integridad:** los datos almacenados por la organización se almacenarán y tratarán de manera que se garantice su integridad.
  + **Principio de eficiencia:** la organización conseguirá la mejor relación entre los resultados obtenidos por la misma y los recursos utilizados para ello.
  + **Principio de transparencia:** la organización ofrecerá públicamente informes sobre la gestión de la organización, preservando la confidencialidad. A su vez ofrecerá informes sobre la gestión de la seguridad de la organización.
  + **Principio de comunicación:** la organización comunicará a sus empleados sus roles y responsabilidades en cuanto a la seguridad de la empresa.
  + **Principio de compliance:** la organización garantizará el cumplimiento normativo vigente.
* **Organización de la seguridad**
* **ESTRUCTURA**

La seguridad de la organización puede distinguirse en dos aspectos: seguridad física y seguridad lógica.

* **Seguridad física:** se encarga de proteger la infraestructura de la organización ante posibles desastres naturales, incendios, inundaciones, robos, etc.
* **Seguridad lógica:** se encarga de complementar a la seguridad física, pero en este caso enfocado al software, protegiéndolo de robos, pérdidas de datos, virus, ciberataques, etc.
* **RESPONSABILIDADES**
* El director general es el mayor responsable de la seguridad de la organización, en conjunto con el departamento de seguridad.
* El Departamento de Seguridad se encargará de asegurar que la seguridad se gestione adecuadamente en toda la organización. Son los responsables de la seguridad den toda la organización
* Cada director de departamento será el responsable de la seguridad de los empleados que trabajan para ese departamento.
* El Departamento de Seguridad asesorará al Director General para que este tome las decisiones correctas.
* Todos los empleados poseen responsabilidad sobre la seguridad de los mismos, y deberán actuar de la forma correcta para evitar problemas.

Existirá un proceso de comunicación continuado entre el departamento de Seguridad y los demás departamentos, con el objetivo de proteger toda la organización de manera adecuada. Cada director de departamento identificará los activos críticos.

* **AUDITORÍAS**

Con el objetivo de cuantificar el nivel de seguridad de la información, se realizarán auditorías periódicas (mínimo anualmente).

* Auditorías de **Pentesting:** se simularán ataques a la organización para comprobar la efectividad de la seguridad y desarrollar mejoras.
* Auditorías de **Vulnerabilidades:** se utilizarán herramientas de búsqueda de vulnerabilidades, con el objetivo de identificarlas para posteriormente desarrollar medidas que permitan su eliminación.
* Auditorías de **Seguridad:** ISO 27001, CAIQ, etc.
* **Revisión de auditorías**

| **Tipo** | **Autor de la auditoría** | **Fecha Inicio** | **Fecha Fin** | **Referencias** | **Resultado** |
| --- | --- | --- | --- | --- | --- |
| Pentesting | Secure S.L. | 18/12/2022 | 18/1/2023 | Véase apartado ‘Referencias’ | **✅** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

* **Marco normativo**

Atendiendo al contexto de la organización, aplica la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ya que la empresa trata con información de sus clientes. Por lo tanto, la organización estará obligada a cumplir con los siguientes puntos, entre otros:

* **Exactitud de los datos.** Se recogerán los datos exclusivamente necesarios para el fin con el que se utilizan y no podrán destinarse a ningún otro. Cuando dejen de ser necesarios, serán eliminados.
* **Derecho de información en la recogida.** Cuando se recojan los datos mediante un formulario, constará el hecho de que van a ser incorporados a un fichero y se especificará el fin con el que se recogen. Deberá identificarse también al responsable de esa información y añadir que el que proporciona los datos tiene derecho a cancelar o rectificar los mismos.
* **Consentimiento del afectado.** El que proporciona los datos deberá consentir en su uso para el fin expuesto. Ese consentimiento podrá ser revocado cuando exista causa justificada para ello.
* **Datos especialmente protegidos.** No deben recabarse datos de nivel medio y alto a menos que sean estrictamente necesarios para la actividad. Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias, por lo que cuando se proceda a recabar el consentimiento al tratamiento de estos datos se advertirá al interesado acerca de su derecho a no prestarlo.
* **Deber de secreto.** El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos. Estas obligaciones subsistirán incluso después de finalizar sus relaciones con el titular del fichero.
* **Comunicación o cesión de datos.** Los datos de carácter personal sólo podrán ser comunicados o cedidos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
* **Seguridad de los datos.** El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. En el caso de ficheros informáticos, el responsable deberá redactar un Documento de Seguridad que deberán seguir todos los que manejen la información. La Agencia de Protección de Datos dispone de un modelo en su página web.
* **Notificación de ficheros.** El responsable o titular debe notificar los ficheros a la Agencia de Protección de Datos antes de su creación.
* **Planes estratégicos**

A continuación, se muestran una serie de planes estratégicos que deberán desarrollarse con el objetivo de garantizar la seguridad de la organización y reducir los posibles riesgos a los que se enfrenta la empresa. Para la implantación de estos planes se identificarán una serie de controles con los que se revisará la política global de seguridad.

Estos controles serán clasificados según:

* **Alcance:**
  + Usuarios (USU): aplica a los trabajadores de la empresa y sus clientes.
  + Datos (DAT): aplica a los datos tratados por la organización.
  + Tecnología (TEC): aplica a la tecnología utilizada por la organización.
  + Gestión (GES): aplica a los procesos de gestión de la empresa.
* **Complejidad:**
  + Básico (B): el esfuerzo y los recursos para implantarlo son asumibles.
  + Avanzado (A): el esfuerzo y los recursos para implantarlo son considerables.
* **Tabla de controles**

En la siguiente tabla se muestra un conjunto de controles que desarrollarán con el objetivo de garantizar la seguridad empresarial. Estos controles podrán tener dos estados:

* **Implantado (✅):** el control verifica que se ha implantado un plan en la política global de seguridad.
* **No implantado (❌):** significa que no se ha desarrollado ningún plan estratégico que cumpla con ese control, por lo que la política deberá ser revisada y actualizada para cumplir con el control determinado.
* **En proceso de implantación (🔁):** significa que se ha definido un plan estratégico que se encuentra en proceso de implementación.
* **En proceso de actualización (🔜):** se refiere a que el plan estratégico implantado está en proceso de renovación o actualización.

| NIVEL | ALCANCE | CONTROL | | ESTADO |
| --- | --- | --- | --- | --- |
| A | GES | Identificar el contexto de la organización | | **✅** |
| A | GES | Desarrollar una política global de seguridad acorde al contexto de la organización | | **✅** |
| A | GES | Definir los proyectos a realizar | | **✅** |
| A | GES | Clasificar los proyectos según su importancia. | | **✅** |
| B | GES | Aprobar la política global de la organización | | **✅** |
| B | GES | Implantar la política global de la organización | | **🔁** |
| A | USU | Comunicar la política global de la organización a todos las personas pertenecientes a la misma | | **✅** |
| A | GES | Evaluar la política global de la organización | | **🔁** |
| A | GES | Desarrollar nuevos proyectos que permitan reducir riesgos potenciales | | **✅** |
| A | TEC, DAT | Identificar activos críticos | | **✅** |
| A | USU, DAT, TEC, GES | Realizar un análisis de riesgos | | **✅** |
| A | GES, DAT, TEC | Establecer un apetito de riesgo | | **✅** |
| A | USU, DAT, TEC, GES | Desarrollar, implantar y evaluar un plan de gestión de incidentes | | **🔁** |
| A | GES, TEC, USU, DAT | Desarrollar, implantar y evaluar un plan de gestión de auditorías | | **🔁** |
| B | GES, USU, DAT, TEC | Definir roles y responsabilidades para garantizar la seguridad empresarial | | **✅** |
| A | USU, DAT, GES | Desarrollar, implantar y evaluar un proyecto de confidencialidad | | **🔁** |
|  | | | | |
| REVISADO POR | | APROBADO POR | NOTAS | FECHA |
| Departamento de seguridad HuescaTelecom | | Director General HuescaTelecom |  | 1/03/2023 |