Normativa Global de Seguridad  
HuescaTelecom



Departamento de Seguridad HuescaTelecom  
2023

* **Introducción**

El objetivo de la normativa es establecer una serie de acciones que permitan garantizar la seguridad de la organización, según los planes especificados en la política global de seguridad.

Este documento aplica a todas las personas y elementos que tengan relación con la organización (trabajadores, tecnologías, clientes proveedores, datos tratados, etc). La normativa será evaluada y actualizada al menos anualmente o cuando ocurra algún incidente de seguridad.

Las actividades a desarrollar serán definidas, implementadas y evaluadas por el departamento de seguridad de la organización, responsable de las modificaciones de la normativa. Cualquier cambio en la normativa deberá ser aprobada por el equipo directivo.

Esta normativa será comunicada a los trabajadores, proveedores y clientes de la organización, ya que el principio de transparencia es uno de los pilares fundamentales de la organización.

* **Tabla de revisión**

| **Fecha** | **Actualizado/revisado por:** | **Versión** | **Vigente hasta:** | **Notas** | **Comunicado** |
| --- | --- | --- | --- | --- | --- |
| 12/2/2023 | Departamento Seguridad | 1.0 | 12/2/2024 |  | ✅ |
|  |  |  |  |  |  |

* **Referencias**
  + [Marco Normativo HuescaTelecom](https://docs.google.com/document/u/0/d/1GE4BrZm39-_Rax-_XpAIt_9A7pkM1-M_XHETDCSh7Zk/edit)
  + [Política Global de Seguridad 2023 - HuescaTelecom](https://docs.google.com/document/u/0/d/1drU9j0SBh8V19MoflmnpJAjqsvAQCJ06SvFxepK6EaI/edit)
  + [Activos y Análisis de riesgo v2](https://docs.google.com/spreadsheets/u/0/d/1rTQhdNv3sx8eRLwe46Kkz-E-3GxR3wsusPezbYHmk74/edit)
* **Organización de la seguridad**

En este apartado se identificará la función de cada departamento, las responsabilidades y obligaciones de los empleados de la organización y la gestión de los proveedores.

RACI

**Veáse:** [Organización Seguridad - Normativa Global de seguridad](https://docs.google.com/spreadsheets/u/0/d/1tdDNP8z-4_tBRnfO-MUB8nN4529Q6EbFx2S6Rm-16gU/edit)

En el siguiente esquema se muestra el **nivel global de responsabilidad** en cuanto a la seguridad de la organización:

****

* **Objetivos de control**

Según los controles establecidos en la [Política Global de Seguridad 2023 - HuescaTelecom](https://docs.google.com/document/u/0/d/1drU9j0SBh8V19MoflmnpJAjqsvAQCJ06SvFxepK6EaI/edit), se definirán los siguientes puntos claves:

* **Identificar el contexto de la organización:** Se formará un equipo de trabajo que realizará un análisis detallado del estado de la empresa en materia de seguridad. Se tendrán en cuenta los siguientes aspectos:
  + Definir el alcance de la Política Global de Seguridad (PGS).
  + Definir los roles y responsabilidades de cada persona implicada en la organización.
  + Valorar el estado de la organización.
  + Realizar una evaluación del cumplimiento de la Política Global de seguridad, con el objetivo de desarrollar nuevas medidas y actualizar las medidas actuales.
  + Definir los objetivos de la Política Global de seguridad en la organización, identificando los aspectos más críticos para la organización.
  + Se evaluará el nivel de implantación de los controles establecidos, con el objetivo de desarrollar más a fondo los controles con una implantación menor.
  + Se identificarán los riesgos a los que está sometido la empresa mediante un análisis de riesgos, donde:
    - Se identificarán los activos de la organización.
    - Se identificarán los activos críticos de la organización.
    - Se identificarán posibles amenazas.
    - Se identificará la probabilidad de que estas amenazas ocurran.
    - Se establecerá el impacto de cada amenaza sobre los activos.
    - Se identificarán los ‘puntos’ más peligrosos de la organización.
  + De esta manera la organización conocerá cuales son los riesgos en los que se debe centrar, y se establecerá un apetito de riesgo.
  + Una vez realizado el análisis de riesgos, se establecerán medidas para mitigar el riesgo
* **Desarrollar una Política Global de seguridad acorde al contexto de la organización:** Para desarrollar una PGS acorde al contexto de la organización, se deberá tener en cuenta el ámbito de la organización, la gestión, la infraestructura, las tecnologías utilizadas, los objetivos de la PGS, etc.
* **Definir los proyectos a realizar:** Una vez identificados los riesgos a los que está sometida la organización, se definirán los proyectos y estrategias a implantar con el objetivo de reducir el riesgo. Entre estos proyectos, se podrán encontrar, entre otros, los siguientes:
  + Concienciación de los empleados de la organización.
  + Corrección de los controles implantados.
  + Gestión de los riesgos más importantes a los que está sometida la organización.
  + Implantación de controles que no han sido implantados en la empresa
  + Etc.
* **Clasificar los proyectos según su importancia:** Una vez identificadas las medidas a realizar, se clasificarán según su importancia con el objetivo de priorizar las medidas. Para ello, se tendrá en cuenta:
  + Nivel de riesgo.
  + Apetito de riesgo.
  + Obligaciones de la organización, en términos legislativos.
  + Se identificarán las acciones que requieran un mayor grado de colaboración entre los miembros de la organización.
  + Se identificarán las medidas destinadas a reducir el riesgo de los activos críticos de la organización.
  + Se identificarán los recursos necesarios para la implantación de las medidas establecidas.
* **Aprobar la política global de la organización:** Una vez creada una versión inicial de la PGS, ésta deberá ser aprobada por el Director General de la organización.
* **Implantar la política global de la organización:** Una vez aprobada la PGS, se implantará ajustándose a la gestión empresarial. Se deberá:
  + Comunicar la PGS a todos los empleados, clientes y proveedores de la organización.
  + Asignar los roles y responsabilidades a las personas implicadas en la organización.
  + Establecer la vigencia de la PGS.
  + Establecer un proceso de evaluación de la PGS.
  + Establecer un proceso de actualización de la PGS (al menos anualmente).
  + Documentar las medidas realizadas y el resultado de las mismas.
* **Comunicar la política global de la organización a todos las personas pertenecientes a la misma:** Una vez implantada la PGS, será necesario comunicar las medidas y proyectos a realizar y los objetivos de la misma. Este proceso de comunicación será:
  + El departamento de Seguridad comunica el PGS al Director General, que lo aprobará.
  + Una vez aprobado, los responsables de seguridad se reunirán con los directores de departamento, con el objetivo de comunicarles la PGS.
  + Los directores de departamento comunicarán a los empleados de su departamento la PGS.
  + Se establecerá un canal de solicitudes y quejas para que cualquier empleado pueda informar de cualquier incidente y/o sugerencia.
* **Evaluar la política global de la organización:** Se deberá evaluar, controlar y verificar el correcto funcionamiento de las medidas establecidas acorde con la PGS. El objetivo de esta evaluación es implantar un proceso de mejora continuada de la PGS, con el objetivo de garantizar la seguridad de la organización.
* **Desarrollar nuevos proyectos que permitan reducir riesgos potenciales:** resultado del proceso de evaluación de la PGS, se identificarán posibles ámbitos en los que no existan controles y medidas establecidas, con el objetivo de desarrollar nuevos proyectos que aumenten la seguridad de la organización. A su vez, se actualizarán las medidas existentes con el objetivo de la mejora de las mismas.
* **Identificar activos críticos:** Se deberán identificar los activos críticos de la organización, con el objetivo de priorizar el desarrollo de medidas para los mismos. De esta manera se aumentará el nivel de seguridad empresarial.
* **Realizar un análisis de riesgos:** Una vez identificados los activos, se realizará un análisis de riesgos teniendo en cuenta las amenazas a las que se enfrenta la organización y la probabilidad de que estas ocurran. Una vez obtenidos los resultados, se definirán los activos con mayor riesgo, con el objetivo de desarrollar las medidas oportunas para reducir el riesgo.
* **Establecer un apetito de riesgo:** Es necesario identificar el riesgo aceptable por la organización. Con esto se obtiene información sobre si los diferentes riesgos están en el margen aceptable por la empresa.
* **Desarrollar, implantar y evaluar un plan de gestión de incidentes:** Se implementará un plan de gestión de Incidentes, es decir, como la organización debe actuar para recuperarse de cualquier incidente. Este debe ser un proceso de mejora continuada, es decir, deberá estar en constante evaluación con el objetivo de garantizar la seguridad de los activos y combatir posibles nuevos riesgos.
* **Desarrollar, implantar y evaluar un plan de gestión de auditorías:** Para aumentar el nivel de seguridad de la organización, será necesario implementar un proceso de auditorías, que podrán ser internas o externas, con el objetivo de descubrir vulnerabilidades en la organización para posteriormente desarrollar medidas para evitar estas vulnerabilidades. Las auditorías podrán ser:
  + 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:** Estas auditorías consisten en comprobar si en la organización se han implementado una serie de controles, o cual es el estado de las Políticas de Seguridad de la organización (ISO 27001, CAI, etc.).

Cabe destacar que estas auditorías deberán repetirse periódicamente, y el resultado de las mismas debe ser documentado y comunicado a los miembros de la organización.

* **Definir roles y responsabilidades para garantizar la seguridad empresarial:** Para una correcta gestión de la seguridad de la organización, deben definirse los roles y responsabilidades de todas las personas implicadas con la organización,
  + Véase: [Organización Seguridad - Normativa Global de seguridad](https://docs.google.com/spreadsheets/u/0/d/1tdDNP8z-4_tBRnfO-MUB8nN4529Q6EbFx2S6Rm-16gU/edit)
* **Desarrollar, implantar y evaluar un proyecto de confidencialidad:** Deberá implantarse un sistema de gestión de la confidencialidad de la información empresarial. Los empleados deberán firmar un acuerdo de confidencialidad con el objetivo de evitar filtraciones de información sobre datos empresariales, proyectos de I+D+i, etc.
* **Véase:**  [Activos y Análisis de riesgo v2](https://docs.google.com/spreadsheets/u/0/d/1rTQhdNv3sx8eRLwe46Kkz-E-3GxR3wsusPezbYHmk74/edit)**, Hoja ‘Controles, herramientas y procesos’**
* **Plan de actuación ante incidentes de seguridad**

En caso de que la organización sufra algún incidente de seguridad, se realizarán las siguientes acciones:

1. Se formará un grupo entre el Director General, los responsables de seguridad y los directores de cada departamento. También formarán parte los trabajadores del departamento de informática.
2. Se identificará el problema.
3. Se aislará el problema todo lo posible, evitando la interrupción del servicio de la organización.
4. Se comunicará el problema a los empleados de la organización.
5. Se comunicará el problema a los proveedores y clientes de la organización.
6. Todos los empleados de la organización trabajarán conjuntamente para la resolución del problema.
7. Desde la organización se debe mostrar tranquilidad y paciencia, con el objetivo de mostrar una buena imagen a clientes y proveedores.
8. Se comunicará el incidente a las autoridades pertinentes (INCIBE, Guardia Civil, Polícia Nacional, etc.)
9. Una vez identificado el problema, se desarrollarán medidas para mitigarlo acorde con el contexto de la organización y la continuidad de negocio.
10. Una vez mitigado el problema, se actualizará la Política Global de Seguridad y la Normativa Global de Seguridad, con el objetivo de evitar (si es posible) que se vuelva a repetir el problema, o al menos reducir el impacto.