VIEWNEXT
AN IBM SUBSIDIARY

# FORMACIÓN
# SEGURIDAD Y PRIVACIDAD DE DATOS
# GDPR

VERSIÓN 3.3

IBERDROLA

VIEWNEXT
AN IBM SUBSIDIARY

La protección de datos se fundamenta en prácticas, principios y derechos fundamentales que las empresas activan con el objetivo de garantizar y proteger la información personal de sus clientes y asegurar su manejo y control.

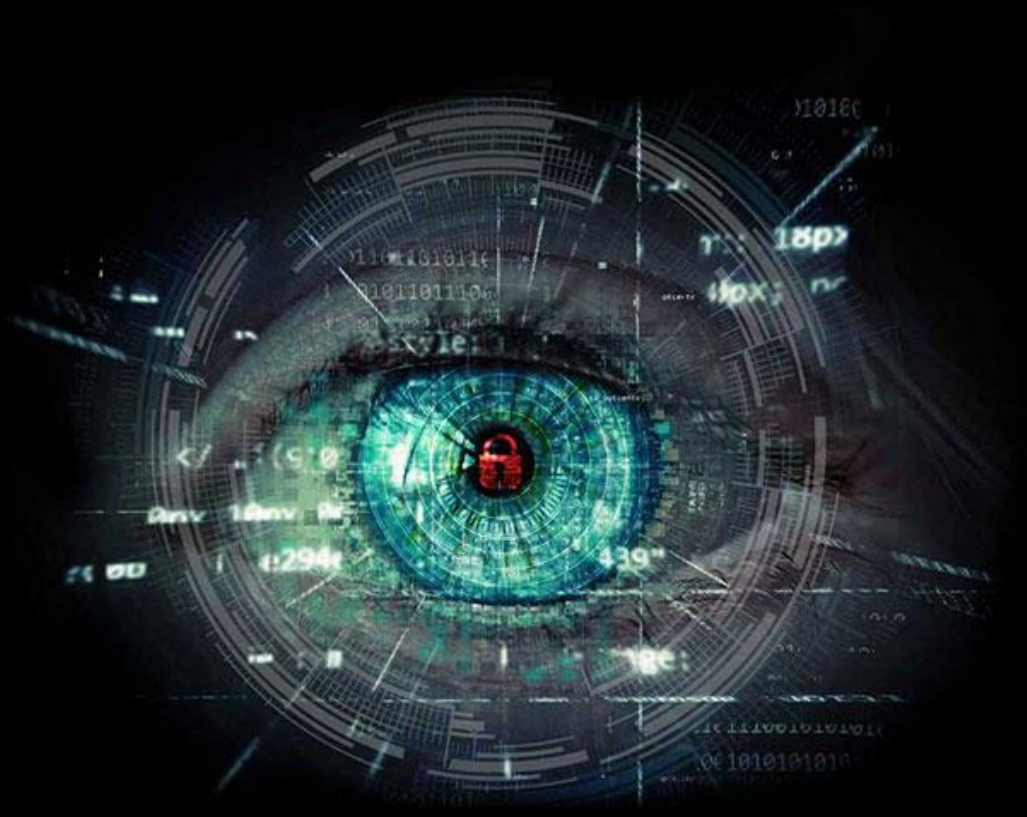
La protección de datos forma parte del día a día para Viewnext, que toma medidas para proteger la información tanto de clientes, como corporativa para dar cumplimiento a la Ley GDPR y a los requisitos de seguridad que tiene establecidos el cliente.

> Objetivo: Garantizar sin fisuras, la privacidad y seguridad de la Información del Proyecto



IBERDROLA

# Índice





VIEWNEXT
AN IBM SUBSIDIARY


# Introducción

- Objetivos y Definiciones
- Importancia del SyPD.
- Responsabilidades

Formación Específica Seguridad y Privacidad de datos

VIEWNEXT
AN IBM SUBSIDIARY

## Objetivos de la Formación

- Instruir a todos los miembros del proyecto para que cumplan las políticas de Viewnext y los requerimientos de SyPD del contrato del cliente.
- Asegurar que todos los miembros del proyecto conozcan las políticas y requerimientos de seguridad y privacidad de datos (SyPD - GDPR) de Viewnext específicos de este proyecto.

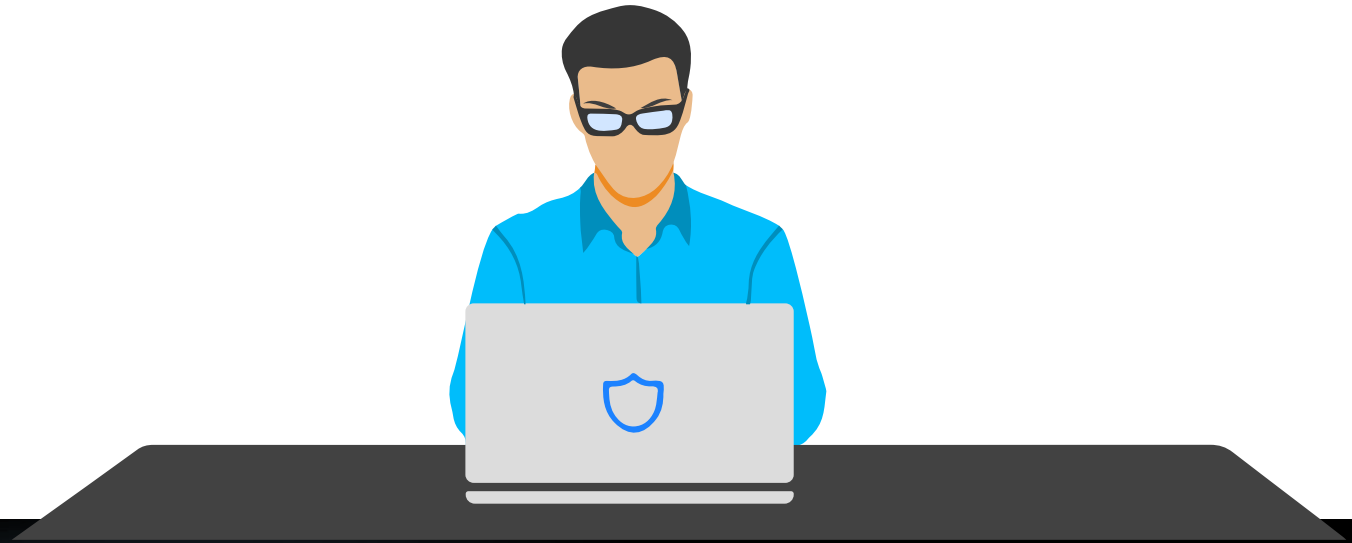
# Objetivos & Definiciones

## Seguridad

La Seguridad es un conjunto de prácticas que se emplean a través de las personas, procesos y tecnología para proteger la información, con el fin de minimizar el riesgo de filtración de datos o tratamientos incorrectos que pongan en compromiso la seguridad de esta información. La seguridad ayuda a proporcionar; confidencialidad, integridad de los datos, disponibilidad de datos, autenticación….

## Privacidad

Capacidad de las personas para determinar cuándo, cómo y en qué medida la información sobre ellos puede ser utilizada o revelada a terceros.



# Objetivos & Definiciones

## Información Personal IP o PI

Cualquier información que identifique o pueda ser utilizada para identificar, contactar, o localizar a la persona a quien pertenece dicha información.

Una persona física identificable es aquella que puede identificarse, directa o indirectamente, en particular por referencia a un identificador, por ejemplo:

Nombre, Apellidos, Número de identificación, datos de ubicación, etc.

## Información Personal Sensible IPS o SPI

Aquella que tiene riesgos potenciales de mal uso y podrían utilizarse para perjudicar a una persona.

En esta categoría estarían datos relacionados con la salud, religión, origen racial, condenas penales, etc.


## Información Negocio Sensible INS o BSI

Se trata de información protegida por el cliente o por otra compañía y que es importante para su negocio.

La exposición impropia o un uso inadecuado de esta información puede causar algún tipo de daño.

Viene determinada por el cliente.

# Objetivos & Definiciones

## GDPR

Se trata de un reglamento que establece los requisitos específicos para empresas y organizaciones sobre recogida, almacenamiento y gestión de los datos personales.

Se aplican tanto a las organizaciones europeas que tratan datos personales de ciudadanos en la UE como a las organizaciones que tienen su sede fuera de la UE y cuya actividad se dirige a personas que viven en la UE.

El GPR se aplica cuando:

- la empresa trata datos personales y tiene su sede en la UE, independientemente de dónde se traten de hecho los datos.
- la empresa tiene su sede fuera de la UE pero trata datos personales relativos a ofertas de bienes o servicios a ciudadanos en la UE, o supervisa el comportamiento de ciudadanos en la UE.

## TOMs >> Medidas Técnicas y Organizativas

Medidas que acreditan y garantizan la Seguridad de los datos personales que se tratan en una empresa, con el fin de asegurar la integridad y confidencialidad de los datos.

# Importancia del SyPD

La falta de protección de la información personal (IP/IPS/INS) de los sistemas cliente pueden afectar a Viewnext e IBM. El número de leyes y regulaciones en esta área continúa creciendo, y las violaciones se informan en los titulares de los medios de comunicación casi todas las semanas.

## ¿Puede realmente ocurrir una violación? ¿Qué efecto puede tener?

- Impacto negativo en la reputación de las marcas  Viewnext e IBM.
- Publicidad negativa.
- Pérdida de confianza en las relaciones con nuestros clientes.
- Pérdida de posiciones competitivas de Viewnext e IBM.
- Pérdida de negocios futuros.
- Litigios potenciales e investigaciones.
- Posibles sanciones por no cumplir con las leyes y sus reglamentos.
- Desperdicio de recursos valiosos.

# Responsabilidades Generales

## ¿Qué debo hacer como miembro del proyecto?

1. Completar la Formación Específica del proyecto.
2. Comprender la política de Seguridad y Privacidad de Viewnext y requerimientos específicos del cliente.
3. Comprender y participar en los controles de “Data Security & Privacy” (SyPD).
4. Adherirme a las políticas de Seguridad del puesto de trabajo (Workplace Security (WPS)) aplicables.

Para cumplir correctamente con los acuerdos en materia de SyPD debo tener presente que, como miembro del proyecto, debo:

- Reportar cualquier brecha de datos real o la sospecha de una brecha a mi responsable.
- Gestionar riesgos relacionados con el tratamiento de IP, IPS e INS.
- Hacer el entorno de trabajo seguro en casa y/o entornos remotos.
- No utilizar servicios públicos de ‘cloud’ como p.ej. Google Docs, Dropbox, Apple iCloud, etc para crear, almacenar, enviar, realizar back up o compartir información confidencial de nuestras empresas o del cliente.
- Evidenciar que he completado la formación.


# Normativa AMS Iberdrola

- Normas de Obligado cumplimiento IBR
- Atención Especial Posibles Riesgos

IBERDROLA

## Formación Específica Seguridad y Privacidad de datos

VIEWNEXT
AN IBM SUBSIDIARY

# Normas de Obligado Cumplimiento

IBERDROLA

VIEWNEXT
AN IBM SUBSIDIARY

Como miembro del equipo de proyecto, debes cumplir de forma obligatoria las siguientes normas:

## Norma 0

Debes comunicar a tu responsable cualquier incumplimiento que detectes de la normativa vigente, en todas sus dimensiones: GENÉRICA VIEWNEXT – PUESTO DE TRABAJO Y/O ESPECÍFICA DEL PROYECTO. Tu responsable lo gestionará de acuerdo con el Proceso de Gestión de Riesgos y Problemas establecido en la Metodología.

## Norma 1

Con el fin de impedir el acceso a los equipos, soportes y otros repositorios de información por parte de personal no autorizado, está prohibido compartir la tarjeta identificativa para acceso a tornos o utilización de impresoras.

## Norma 2

Está terminantemente prohibido tratar datos de carácter personal de IBERDROLA. Si visualizas este tipo de información, trasládalo de forma urgente a un responsable.

## Norma 3

No debe dejar el equipo desatendido, aunque se trate de una breve pausa, sin antes proceder a su desconexión, suspensión o cualquier otra medida que bloquee el equipo e impida su uso por parte de otro usuario:

CTRL + ALT + SUPR


## Norma 4

Está prohibido dejar el equipo encendido a la finalización de la jornada laboral, sin la debida autorización otorgada por el Departamento de Sistemas.

## Norma 5

Está terminantemente prohibido alterar la configuración relativa a los mecanismos de seguridad para el establecimiento de la conexión remota a la red de IBERDROLA.

## Norma 6

Cualquier necesidad de acceso a sistemas o aplicaciones de IBERDROLA debe ser solicitada a un responsable, que coordine y autorice la gestión de accesos sobre datos y recursos a IBERDROLA.

## Norma 7

Las contraseñas y los permisos de acceso a los recursos de IBERDROLA son personales e intransferibles, manteniéndose así la confidencialidad de las contraseñas de acceso a los módulos, que no se revelarán a terceros.

IBERDROLA se reserva el derecho de controlar y auditar la actividad de los usuarios en sus sistemas y entornos, así como de suspender, en su caso, los accesos concedidos si lo considera necesario.

Con carácter particular, IBERDROLA auditará aquellos accesos que puntualmente se concedan al entorno productivo, al personal que desempeñe tareas relativas a los servicios sobre los sistemas a los que se refiere el contrato.

# Normas de Obligado Cumplimiento

IBERDROLA

VIEWNEXT
AN IBM SUBSIDIARY

## Norma 8

Está prohibido extraer datos IP, IPS, INS, depositarlos en un servidor o enviar a un usuario vía file transfer o anexado en un correo así como el uso de dispositivos externos de memoria para transportar información, salvo expresa autorización y por escrito de IBERDROLA.

## Norma 9

Está prohibido almacenar IP, IPS, INS, de IBERDROLA en los equipos portátiles, salvo que en virtud del servicio a prestar, fuese necesario, en cuyo caso se debe proteger mediante cifrado u otro mecanismo que garantice que la información no sea inteligible ni manipulada por personal no autorizado.

## Norma 10

Los soportes en papel deben ser destruidos una vez dejen de ser necesarios. El mecanismo de destrucción ha de garantizar que la información no se pueda recuperar.

## Norma 11

Viewnext mantiene debidamente protegidos los equipos frente a software malicioso. Está terminantemente prohibido alterar cualquier configuración de seguridad en los equipos.

## Norma 12

Está terminantemente prohibido utilizar datos reales en entornos distintos a los de Producción. Si se prevé copiar IP, IPS o INS, desde los entornos de Producción a otro entorno, éstos deberán ser disociados previamente, garantizando la no identificación.

## Norma 13

En caso de ser absolutamente necesario utilizar datos reales para pruebas, no se podrá hacer sin la autorización expresa y por escrito de IBERDROLA. En tal caso, los datos deberán ser disociados previamente.

## Norma 14

Los ficheros temporales deben ser borrados una vez que hayan dejado de ser necesarios para los motivos de su creación

## Norma 15

No está permitido realizar ninguna copia de seguridad que contenga datos de carácter personal.

## Norma 16

Viewnext mantiene un Procedimiento de Gestión de Incidencias de Seguridad compartido con IBERDROLA. Es obligatorio comunicar a tu responsable cualquier situación que ponga en riesgo la seguridad de los datos. En particular aquellos que deriven de un eventual acceso a datos de carácter personal.

# Normas de Obligado Cumplimiento

## Norma 17

El proyecto está sujeto a inspecciones y auditorías de SyPD: AEPD (Agencia Española Protección Datos), IBERDROLA, Viewnext / IBM, y cualquiera a medida del proyecto.

Es obligatorio facilitar la realización de esos controles y colaborar con las necesidades que el órgano de gobierno requiera

## Norma 18

Es obligatorio cumplir con el plan de acción resultante de una auditoría o inspección, explicado en el punto anterior.

## Norma 19

En cualquier caso, es de obligado cumplimiento guardar secreto respecto a los datos a los que eventualmente pudiesen tener acceso. Este secreto deberá mantenerse aún después de haber finalizado el servicio y en ningún caso se hará uso de los mismos

## Norma 20 * BPO Soporte

El servicio del AMS: BPO Soporte, trabaja de forma autorizada con la finalidad de cumplir con los objetivos del servicio con "Información Confidencial".
En ese caso si eres recurso de BPO Soporte, debes conocer que toda la información relativa a datos económicos, portfolio de sistemas, información de proveedores y, en general, toda la documentación que IBERDROLA pudiera facilitar a Viewnext para la prestación del Servicio o a la que Viewnext pudiera tener acceso cualquiera que sea su formato o soporte debe estar protegida bajo las máximas medidas de seguridad establecidas en el contrato.

## Norma 21

Está totalmente prohibido exponer código fuente propiedad de Iberdrola (tanto desarrollado por Viewnext como por otras empresas) hacia el exterior, esto es, NO se puede subir el código fuente ni cualquier tipo de documentación a repositorios o sitos públicos como puede ser GitHub.

## Norma 22

Está totalmente prohibido tener harcodeados passwords en el código fuente. Todos estos secretos tienen que estar almacenados debidamente en recursos del servidor y usarlos haciendo referencia a los mismos.

## Norma 23

Es obligatorio conectarse a LAN2LAN de Iberdrola a través de Pulse Secure con doble factor de autenticación, incluso estando físicamente en las Oficinas de Viewnext

# Atención Especial Posibles Riesgos

## Administración de usuarios

- Los usuarios deben ser nominales.
- NO compartir ni divulgar ID de usuarios ni contraseñas.
- Al cambiar asignaciones o roles, la PMO y el Responsable se deben asegurar que la cancelación se hace de manera correcta junto con los ID de usuarios que no son necesarios.

## Acceso al entorno de Producción

- Los accesos a producción son proporcionados por Iberdrola.
- Los accesos de escritura, deben ser nominales, temporales y solamente para el diagnóstico y resolución de errores o problemas.
- Deben solicitarse a través de la herramienta de gestión de incidencias (IT Now) quedando constancia de la aprobación del cliente.

## Requerimientos de seguridad del cliente

- Si el miembro del equipo va a tener acceso a aplicaciones de Iberdrola, se le gestionará dicho acceso y dispondrá de un número “Expediente”, que es el usuario de red de Iberdrola.
- La PMO Iberdrola enviará la “Normativa de uso aceptable de la Ciberinfraestructura de Iberdrola “ que el miembro del equipo deberá devolver firmada.

## Administrar la Separación de Tareas

- No se debe tener acceso a desarrollo o pruebas ni a producción para la misma aplicación.
- Cuando existen excepciones, se requieren controles secundarios.
- Si se da este caso, consulta siempre a tu responsable.


# GDPR

- TOMs & Acceso a Datos IP/IPS/IPN
- Aplicaciones/Entornos
- Workplace Security

## Formación Específica Seguridad y Privacidad de datos

VIEWNEXT
AN IBM SUBSIDIARY

# Medidas Técnicas y Organizativas TOMs

*Recuerda!!*
*Dispones de la definición y objetivos de GDPR y TOMs en la Slide 8.*

## Requerimientos legales y/o regulatorios >> TOMs del AMS Iberdrola

- Se dispone de procesos oficiales aprobados y en continua actualización de 1. Gestión de Riesgos & Problemas, 2. Incidencias de Seguridad y 3. Gestión de Vulnerabilidades en la Metodología del Proyecto, que pueden consultarse en todo momento en el Portal de Gestión del Conocimiento KM.
- Se evalúan y actualizan permanentemente los riesgos del proyecto relacionados con el procesamiento de datos personales.
- Se ha creado y se mantiene un Inventario de los datos personales del cliente, y todos los elementos relacionados con la seguridad.
- Se gestionan los Accesos de los usuarios a los entornos técnicos del proyecto según procedimientos establecidos y aprobados.
- Se gestionan los Accesos privilegiados e ID de usuario compartidos bajo el procedimiento específico establecido aprobado por el cliente.
- Se gestiona el Acceso a la red de VIEWNEXT de forma segura junto con todas las medidas técnicas lógicas y físicas establecidas.
- El usuario se compromete a emplear el uso de cifrado, pseudonimización y / o anonimización de datos personales del cliente en procesamiento de datos cuando corresponda.
- Se deben implementar controles de seguridad en las estaciones de trabajo que pudieran procesar eventualmente datos personales del cliente.

# Acceso a Datos IP / IPS / INS

Todos los miembros del proyecto debemos CONOCER qué información está autorizada por el cliente y la naturaleza de las operaciones permitidas.

Consulta con tu Responsable cómo obtener esta información en función de las Aplicaciones a las que te concedan acceso.


El proyecto AMS, es susceptible de acceder a los datos de carácter personal autorizados por el cliente en el contrato. Los datos de carácter personal autorizados por Iberdrola, han sido comunicados a Viewnext mediante dos listados:

1. Tipos de datos personales
2. Categorías de interesados (a los que pueden hacer referencia dichos tipos de datos)

La naturaleza de las operaciones de tratamiento permitidas para dichos datos es:

- Consulta
- Recogida: reciben direcciones de correo electrónico
- Registro: almacenan información de la dirección de correo en la herramienta de envío de mails
- Utilización: se envía un mail a la dirección que ha recibido.
- Adaptación o modificación
- Extracción

# Acceso a Datos IP / IPS / INS

Es importante conocer las siguientes situaciones que pueden darse en el envío de información:

- Se utilizarán datos personales tipo dirección de email, de cuentas recibidas por mail, solo para realizar los envíos de correo electrónico bajo los criterios/requisitos que Iberdrola haya establecido en cada momento.

- En todos los casos deberán mantener el carácter confidencial de la información y su responsabilidad, en caso de divulgarla.

**SECURITY** Una vez cumplida la prestación del servicio, se debe devolver a IBERDROLA o destruir, a elección de ésta última, los datos de carácter personal que pudieran encontrarse en poder del prestador del servicio

# Acceso a Datos IP / IPS / INS

Como venimos recordando, la norma general es que NO debe accederse a datos IP/IPS/INS (revisar slide 7 para entender las diferencias), sin embargo es importante conocer las excepciones:

## EXCEPCIONES DE ACCESO

- Accederán a los datos personales las personas autorizadas para llevar a cabo las funciones de cumplimiento del servicio y bajo las instrucciones del cliente.
- Están autorizadas a tratar exclusivamente los datos personales que sean estrictamente necesarios para cumplir los Servicios objeto del Contrato, gestionar incidencias y realizar pruebas de las aplicaciones.
- Se podrán acceder o consultar los datos personales cuando existan necesidades imperiosas para reproducir un error funcional. En caso de que esto ocurra se deberá registrar el motivo en concreto,
- El acceso a datos personales para la resolución de incidencias solo se realizará con autorización y con dicha finalidad.

En ningún caso debe compartirse la información IP/IPS/INS, ni utilizarse para fines distintos a la prestación del servicio.

# Acceso a Datos IP / IPS / INS


## Almacenamiento de Datos

Evita almacenar datos IP/IPS/INS en dispositivos de almacenamiento portátil, copias en papel, etc.

## Advertencia sobre el Uso de los Datos

Los datos personales que pudieran ser incluidos en herramientas de soporte podrían generar problemas con IP/IPS/INS:

- La IP/IPS/INS incluidos en áreas de texto de formato libre, podrían no cumplir con los requerimientos contractuales y reglamentarios, y deben evitarse siempre que sea posible.
- Las personas sin autorización para visualizar los datos, podrían tener acceso a todos los datos en una herramienta o incluidos en documentos creados durante la vida de un proyecto, tipo: Hojas de cálculo, Documentos de texto, Notas, Correos electrónicos, Capturas de pantalla / Screenshots….

## Transferencia de Datos

Al transferir electrónicamente, recuerde encriptar los datos de IP/IPS/INS o utilice protocolos de seguridad estándar de la industria. Si lo hace físicamente limite la distribución a las personas establecidas y definidas en la lista de control de acceso. Use los controles apropiados de encriptado, y transporte a través de líneas seguras o entrega manual.

Al imprimir o enviar un fax, recuerde no dejar desatendido los datos IP/IPS/INS, si es un fax, Incluya una carta de presentación dirigida al receptor. Para todos los casos, verifique que la máquina receptora o impresonar se encuentre en una ubicación segura. Informar a la parte receptora antes de enviar un fax.

# Acceso a Datos IP / IPS / INS

## QUEDA TERMINANTEMENTE PROHIBIDO

El acceso a cualquier otro tipo de dato personal, categoría de interesado y operación de tratamiento distintos a los comunicados por tu responsable y autorizado por el cliente.

## ¿QUÉ DEBO HACER SI IDENTIFICO UN ACCESO A UN NUEVO TIPO DE DATO NO AUTORIZADO?

1. PARAR la actividad y COMUNICAR de inmediato a:

TU RESPONSABLE + DIRECCIÓN DE PROYECTO + OFICINA DE PROYECTOS

2. Ellos deben solicitar AUTORIZACIÓN expresa al cliente sobre el acceso y la finalidad.

3. ESPERAR la confirmación o instrucciones de los responsables.

# Aplicaciones / Entornos

Existe un inventario aprobado por el cliente de la información IP,IPS, INS a la que los miembros del equipo VIEWNEXT tienen acceso, detallando cada sistema y entorno. Es en este inventario deben recogerse, y gestionarse los accesos a las aplicaciones.

Consulta a tu responsable siempre que tengas dudas.

Recuerda:

- Entornos NO productivos: No debe haber datos IP/IPS/INS.
- Producción: Deben detallarse en el inventario del cliente todos los accesos a este entorno

## Gestión y Control de los accesos a Aplicaciones y Entornos:

Los accesos son solicitados por el Director del Proyecto o por el Responsable de área, de acuerdo al Procedimiento de Administración de Usuarios que puede consultarse en la metodología del AMS Iberdrola, en la herramienta de Portal de Gestión del Conocimiento KM.

Los usuarios y sus accesos son revalidados TRIMESTRALMENTE por el cliente y éste puede utilizar controles específicos como puede ser la monitorización de los accesos.

# Aplicaciones / Entornos

## TU RESPONSABILIDAD

- Comprender los requerimiento con respecto a IP/IPS/INS.
- Usar buenas prácticas de seguridad en todo momento. Las áreas clave para poner foco incluyen:
  - Protección de IP, IPS e INS.
  - Gestión de acceso a sistemas y entornos.
  - Separación de tareas.
- Minimizar los riesgos asociados con el acceso a IP/IPS/INS y cumplir las expectativas.
- Cumplir con los requerimientos y procedimientos del proyecto a los que se hace referencia en esta formación.

**Atención**: NO todas las respuestas se ajustan a las diversas situaciones de los proyectos. Para encontrar la respuesta correcta:

1. Pregúntate cuál es la mejor forma de tratar y proteger los datos de los que eres responsable.
2. Ten en cuenta los requerimientos asociados con esa información.
3. Si no estás seguro, pregunta a tu responsable.
4. PIENSA ☺

## TU RESPONSABILIDAD EN TU EQUIPO

Puedes consultar la política corporativa de Viewnext y los controles fundamentales de seguridad y privacidad de datos SyPD relacionados con el uso de tu equipo de trabajo (tanto en oficinas, como en cualquier modalidad de teletrabajo desde casa) en >> Documento SI300, puedes descargarlo en la Intranet de Viewnext.

Las restricciones de uso de otras estaciones de trabajo adicionales, para actividades de usuarios privilegiados, son:

- El uso personal de una estación de trabajo de VIEWNEXT utilizada para realizar actividades privilegiadas está restringido a negocios de VIEWNEXT (solo se permite el uso personal de emergencia).
- No se permite el uso personal de una estación de trabajo provista por el cliente, si no se encuentra autorizado.
- No se pueden usar estaciones de trabajo de propiedad personal.
- No se puede conectar ningún dispositivo de almacenamiento de propiedad personal (HD externo, memoria USB) a una estación de trabajo de usuario privilegiado.

Los recursos subcontratados que tengan acceso a datos del cliente IP/IPS/INS deben usar siempre un equipo proporcionado por Viewnext o cualquier otra empresa del grupo IBM.

VIEWNEXT
AN IBM SUBSIDIARY

# POLÍTICA DE MESAS LIMPIAS Y BUENAS PRÁCTICAS

## Documentación

No dejar documentos confidenciales, ni de información de carácter personal, tanto de Viewnext como del cliente, encima de la mesa, ni en post-its en paredes de corcho, pizarras,...

## Cajoneras, Armarios, Equipos

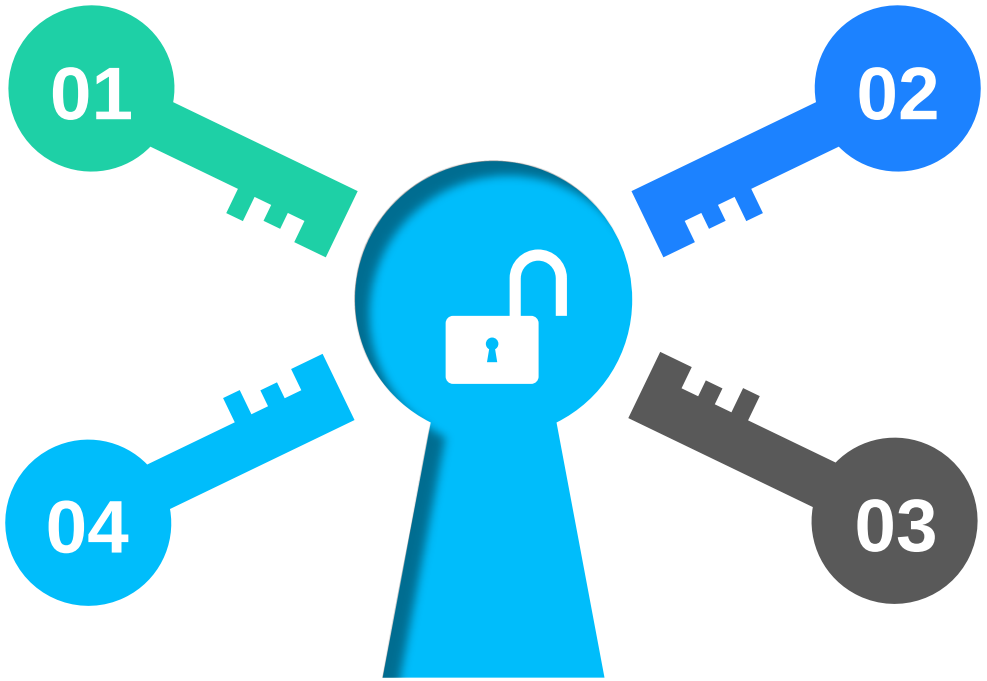
Cerrar los cajones y armarios al final de la jornada laboral.

No dejar llaves en portalápices, bandeja de escritorio, etc...

No dejar passwords escritas en calendarios, trozos de papel, post-its,...

Asegurar el portátil con un cable con candado.

Todos los desktops deberían estar apagados (fuera del horario laboral).




## Confidencialidad

Guardar la información confidencial cuando se abandona el área de trabajo.

La información confidencial debe recogerse sin demora de las impresoras, máquinas de fax,...

Comprobar todos los asistentes a "conference calls" confidenciales.

Mantener seguras las contraseñas y las llaves.

La información confidencial ha de estar adecuadamente etiquetada.

## Transporte

Cuando se transporta un portátil de una ubicación a otra, se han de guardar fuera de la vista en vehículos cerrados.

Recordamos a todos los empleados la obligación de realizar una utilización adecuada y responsable de los recursos informáticos de los que dispone.



IBERDROLA

# Workplace Security

## PROCESO DE REVISIÓN

01

Se realizan inspecciones de cumplimiento de las guías de protección de la información y de los activos periódicamente.

Si durante las inspecciones se encuentra material confidencial o que contenga IP, IPS, INS o se detecta alguna irregularidad en el cumplimiento de la normativa establecida:

02

1. Se cumplimentará un AVISO con el incidente detectado que se dejará en la mesa del empleado. Adicionalmente, será comunicado a la persona a través del registro de No Conformidades Internas (Pain Points en RTC), suscribiendo a su Responsable de Área.

2. Los materiales que constituyan un incidente de seguridad serán confiscados y guardados en un armario cerrado por la persona que lleve a cabo la inspección.

3. Los materiales confiscados no reclamados serán destruidos después de que la Dirección de Proyecto confirme que se ha tratado la incidencia con el empleado. Si se encuentra un portátil que no está asegurado, también será confiscado.

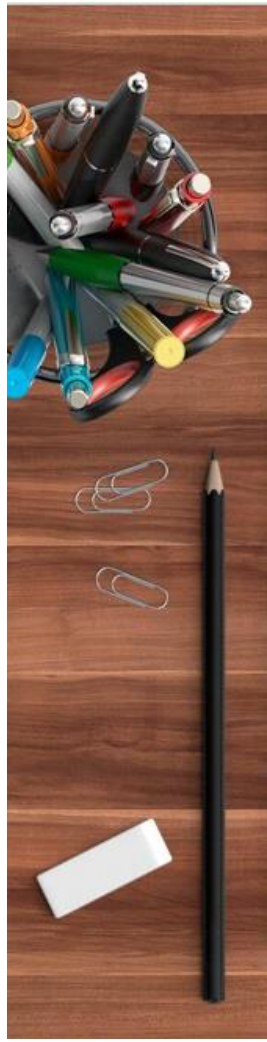
4. En función de la gravedad del incumplimiento, Oficina de Proyectos junto con la Dirección de Proyecto, podrá estudiar si se ha de realizar alguna acción correctiva.

03

Si el equipo de Viewnext está trabajando en edificio del cliente y éste realiza periódicamente inspecciones de WPS, no se consideran sustitutivos de los procesos Viewnext de SPT debiendo llevarse a cabo las políticas aplicables, por parte de la persona del equipo Viewnext designada para ello.

04

Los resultados finales y las posibles acciones correctoras serán reportadas a la Dirección del proyecto.



*En la modalidad Nextworking ante la imposibilidad de realizar auditorías de Workplace Security, el empleado será responsable de disponer de un entorno de trabajo seguro que cumpla la normativa.*


# Consideraciones Finales

Formación Específica Seguridad y Privacidad de datos

VIEWNEXT
AN IBM SUBSIDIARY

# CONSIDERACIONES FINALES

01 Las normas recopiladas en este documento son de obligado cumplimiento para TODOS los integrantes del AMS Iberdrola, tanto empleados Viewnext como personal subcontratado.

02 Todos los empleados Viewnext y el personal subcontratado son responsables de proteger la información confidencial de Viewnext y de IBERDROLA, sin excepción.

03 Deberás confirmar que has leído y comprendido el contenido de esta presentación respondiendo al correo donde fue proporcionada, como una actividad del ON Boarding o bien cuando sea requerido.

04 Cuando seas desasignado de este proyecto, deberás certificar la eliminación de TODA la información del cliente y del proyecto, como una tareas establecidas en el proceso de OFF Boarding.

Ante cualquier duda sobre este documento o el cumplimiento de la normativa del cliente y Viewnext, por favor PREGUNTA!

Responsable de área/servicio – Dirección de Proyecto – Oficina de Proyectos PMO – Seguridad y Privacidad Viewnext

PODRÁN AYUDARTE A RESOLVER TUS DUDAS