ADENDA CONDICIONES TÉCNICAS LOTE 1



GUÍA VIGILANCIA

Marzo 2019

NASERTIC
c) Orcoyen S/N
31011 Pamplona
Tfno: 848 426734

INDICE

1. INTRODUCCIÓN 4

2. NORMATIVAS DEL PUESTO Y TURNOS 5

2.1. Procedimiento a seguir en el control de rondas 8
2.2. Turno de Mañanas 8
2.3. Turno de Tardes 9
2.4. Turno de noches 9

3. FUNCIONES 10

3.1. Control de Acceso al Centro Informático 10
3.1.1 Área de Carga y descarga 15
3.1.2 Control de acceso de visitas a la sala de servidores 16
3.1.3 Acceso a los almacenamientos externos 16
3.1.4 Controles de seguimiento 17
3.1.5 Procedimiento de actuación para los Sábados, Domingos y Festivos 19
3.1.6 Acceso de personas no autorizadas 19
3.1.7 Personal de SEGURIDAD (Vigilantes) 19
3.2. Control de Listados, Correspondencia y Paquetería 19
3.2.1 Listados (entrega, recogida) 19
3.2.2 Control de Correspondencia 20
3.2.3 Entrega de paquetes no certificados 21
3.2.4 Entrega de paquetes o cartas certificadas 21
3.3. Gestión de custodia 22
3.3.1 Control de llaves (entrega y recogida) 22
3.3.2 Ordenadores portátiles 22
3.3.3 Sobres de usuarios de emergencia y protocolo de actuación 23
3.3.4 Custodia del Botiquín del Centro 23
3.4. Correo electrónico 23
3.4.1 Creación de un aviso en el correo electrónico 24
3.4.2 Avisos en el correo electrónicos 25
3.4.3 Crear Archivo de Carpetas Personales (PST) 26
3.4.4 Agregar Archivo de Carpetas Personales (PST) 28
3.5. Buen uso del PC 29
3.6. Control del material de limpieza 29
3.6.1 Limpieza cristales 29
3.6.2 Cajas depositadas en la sala CPD 29
3.7. Vídeo Vigilancia 30
3.8. Gestión del reservado de vehículos 30
3.9. Gestión de siniestros (averías) urgentes 31
3.10. Informes y novedades 32
3.10.1 Informe Diario 33
3.10.2 Informe Mensual de evaluación del estado de los sistemas de seguridad 37
3.11. Notificación de Incidencias 40

4. GESTIÓN Y CONTROL DE SISTEMAS DE SEGURIDAD 40

4.1. Alarmas de Intrusión 40
4.2. Alarmas del Sistema de Refrigeración 41
4.3. Alarmas de detección y extinción de Incendios 41
4.4. Alarmas de control de acceso y vídeo vigilancia 42
4.5. Control de la puesta en marcha del Grupo Electrógeno (cortes de luz) 42
4.6. Aire Acondicionado 43
4.6.1 Temperatura Sala CPD (máxima 27º) 43
4.7. Agua Nebulizada 45
4.8. Compuertas Cortafuegos (armario frente a C. Transf.) 45

5. ANEXO 45

5.1. Ley orgánica de Protección de Datos 15/99 ..... **¡Error! Marcador no definido.**
5.2. Aviso de confidencialidad "DATOS PERSONALES" 45
5.3. Ley Foral 6/2003, de 14 de Febrero, de prevención del consumo de tabaco, de protección del aire respirable y de la promoción de la salud en relación al tabaco. 46
5.4. Avisos a los cuerpos de Seguridad del Estado 47
5.5. Comunicaciones 50
5.5.1 Generalidades 50
5.5.2 Por radio 51
5.5.3 Por teléfono 51
5.5.4 Lenguaje convenido 51
5.5.5 Hechos Ocurridos 52

1. INTRODUCCIÓN

En el siguiente documento se describe las funciones que desarrolla la Unidad de Vigilancia de la empresa.

2. NORMATIVAS DEL PUESTO Y TURNOS

En las dependencias del personal de Seguridad existe un armero. Así mismo no es de extrañar que se presenten en las instalaciones de NASERTIC los cuerpos de Seguridad del Estado para realizar una comprobación del armero y el estado del Edificio, los cuales deberán identificarse cuando accedan a las instalaciones.

Siempre al comenzar la jornada laboral se deberán realizar las siguientes comprobaciones:

- El control de llaves ***se hará siempre durante el relevo*** (siendo responsable de la pérdida de éstas el vigilante saliente). En caso de que se incorpore o falte alguna llave firmar en el Parte de Servicio del vigilante saliente ambos vigilantes (entrante y saliente). Dejando constancia de que se recibe o falta alguna llave, únicamente durante ese día, por parte de todos los vigilantes. Excepto si al día siguiente se incorpora al servicio un vigilante que el día anterior no figurase en el registro.
- Transmisión y recepción de novedades: se realizará durante un solape entre el vigilante entrante y el vigilante saliente de unos diez minutos.
- Verificación del estado de los sistemas de seguridad (central de alarmas…) y otros elementos de trabajo como pueden ser, por ejemplo, tarjetas de visita.
- Cada vigilante dispone de un usuario y contraseña propia para conectarse a su ordenador y abrir las aplicaciones que hará posible llevar de una manera especifica el Control de Accesos. Finalizado su turno de trabajo “será responsable de cerrar su s aplicaciones”.

  Sólo podrán acceder a estas claves el personal de vigilancia que hayan realizado un periodo de aprendizaje en el centro.

NOTA: Para el trabajo en el centro, en supuestos casos extraordinarios, existe un sobre cerrado con un usuario para vigilantes de emergencias.

En el transcurso de la jornada laboral:

- Se dejará constancia en el parte de servicio de acontecimientos a destacar o más relevantes, incidencias y aquellos otros que la dirección trasmita que deban constar (entrega y recogida de llaves, información confidencial que sea facilitada de vigilantes a trabajadores autorizados, entrega y recogida de los dos ordenadores portátiles de la garita vigilantes, todo material que se introduzca o se saque del centro por las empresas de mantenimiento en especial en el acceso a la sala Host, alarmas que se

desconecten temporalmente redactando el motivo y personas para las que se lleva a cabo tal acción, etc.)

- Rondas por el centro dependiendo de la jornada de trabajo a realizar, si es festivo o no, apagar luces, control de temperaturas, etc***. Se realizará la grabación de la Sala CPD siempre que se encuentre gente en dicha zona*** también cuando se tenga ***la puerta de emergencia-calle abierta.***
- En los turnos de noche, festivos y fines de semana, control de presencia cada 60 minutos, mediante lectura del punto de control correspondiente.
- En la unidad de red del departamento se dispone de diferentes informaciones para llevar a cabo el trabajo (informes mensuales de los sistemas de seguridad (siendo redactado de manera rotativa por cada vigilante), tarjetas, etc.)
- Recepción de las visitas derivándolas a las secciones del centro que corresponda, ***debiendo estar convenientemente identificadas y autorizadas.***
- La autorización llega a través del correo electrónico, Base de Datos (una vez grabados sus datos nos aparecerá como ***Personal Autorizado***) o bien, en casos imprevistos (fuera de la jornada laboral, festivos…) contactar a través del móvil con alguna de las siete personas que pueden autorizar el acceso al centro. “Eludir responsabilidades utilizando el tfno. móvil”.
- Nunca se despedirá a nadie porque no conste su autorización, se seguirá el último paso descrito.
- Avisar a Operación cada vez que llegue personal a recoger o entregar listados (Empresa de Mensajería, funcionarios de Hospitales, Agricultura,…)
- Cuando fuese necesario, en el desempeño de su trabajo, el uso de cierto material de oficina (bolígrafos y otros útiles), la solicitud se llevará a cabo a través de la persona encargada de la administración.

NOTA: ***Al finalizar el turno se volverán a dejar los diversos guías, manuales , llaves, etc... En el lugar habilitado para ello con el fin de que no se extravíen y puedan ser localizados por*** todo el personal de seguridad.

NOTA: ***En caso de abandono del puesto de vigilancia, por necesidades de operatividad o cualquier imprevisto,*** *se dejarán* ***cerradas las dos puertas del habitáculo*** *(la puerta de arriba con llave) antes de abandonarlo para realizar cualquier otra tarea. No olvidar* ***recoger las llaves.***

Será de obligado cumplimiento cerrar la puerta principal de acceso, ***queda expresamente prohibido dejar la puerta entornada sin pasar la tarjeta por el lector****. Siempre que efectuemos una salida al exterior deberá quedar registrada en el lector.*

Por precaución y sentido común, antes de ***salir cogeremos la llave de acceso manual*** *al edificio por si fallase el sistema del lector de tarjetas electrónico.*

Será de obligado cumplimiento llevar el teléfono móvil de la Unidad de Vigilancia para que el vigilante pueda ser localizado en todo momento, desviando con anterioridad el teléfono fijo al móvil (*22#0nnnnnnnn#) y comprobando que el desvío funciona correctamente. Quitar el desvío cuando el vigilante se incorpore al puesto de vigilancia (#22#) y comprobarlo.

NOTA: ***Queda terminantemente prohibida la grabación, filmación o realizar cualquier fotografía en las instalaciones de NASERTIC.***

Si se observa a cualquier persona incumpliendo dicha prohibición se avisará al responsable de Seguridad de NASERTIC y se le indicará al infractor.

NOTA: *Queda expresamente* ***prohibido apagar las luces del interior del centro de control*** *durante los turnos nocturnos, festivos y fines de semana.*

Durante dichos turnos, las luces del interior del centro de control permanecerán encendidas y los focos halógenos ubicados en el exterior del cristal de seguridad apagados.

Ante una situación no contemplada en esta ***Guía de Vigilancia***

- Se actuará con profesionalidad y, según cada situación, con iniciativa, lógica, prudencia, comprensión, diplomacia, etc., pero siempre en ***beneficio de la seguridad*** de las personas y bienes.

- Si hay tiempo, se consultará con el ***responsable de Seguridad de NASERTIC.***

2.1. Procedimiento a seguir en el control de rondas

El edificio esta dotado con un de control de rondas, establecido mediante un sistema denominado **ProxyGun.**

La distribución de los puntos de fichaje se realiza en coordinación con el responsable de mantenimiento del edificio, previa autorización del responsable de seguridad del NASERTIC.

En las rondas de inspección y vigilancia se fichará en los puntos de fichaje que se determine en el orden y frecuencia establecidos en la Guía usuario control rondas.

Se establecerán 18 puntos de control. Para más información mirar la Guía usuario control rondas.

NOTA: ***El horario establecido par la ejecución de las rondas es:***

Laborables 6:00 y 20:00

Domingos, Sábados y Festivos a las 8:00 y 20:00

El tiempo establecido para realizar la ronda no debe ser inferior a 15 minutos y no debe superar los 25 minutos. Queda prohibido alterar el orden y la frecuencia establecida de los puntos de fichaje

2.2. Turno de Mañanas

El personal del centro comienza a llegar antes de las 07:00. Alrededor de las 14:00 llega la Sra. de limpieza.

Se enviarán los partes del día anterior.

A petición se abrirá la persiana de Mº Irache, comprobando antes a través de la Base de Datos que quién lo solicita está autorizado.

Control de la temperatura de la Sala CPD, según se explica en el punto 4.6.1. Se realizarán tres capturas entre las 07:00 y las 19:00, en los turnos de mañana de los festivos y fines de semana.

Recepción de las visitas.
Finalizar el servicio creando el parte del turno y dando novedades si existiesen al vigilante entrante (explicarlos de palabra para mejor comprensión).

2.3. Turno de Tardes

El personal del centro comienza a salir a partir de las 14:15 h. aproximadamente.

El personal de seguridad deberá realizar una ronda apagando luces de oficinas que no sean necesarias (una vez se haya marchado el personal de limpieza y no haya quedado algún trabajador inusual), ***comprobando especialmente que la plastificadora (por su riesgo de incendio) y la cortadora hayan quedado apagadas, cerrar las puertas que pudiesen haber quedado abiertas (Sala CPD, condensadoras, UPS, etc.) y verificando el bienestar del centro en general.***

Para más información sobre la ronda mirar la Guía usuario control rondas.

Se recibirá el aviso del cierre de la persiana de Mº Irache, tomando nota de la identidad del solicitante en el parte de servicio.

Control de la temperatura de la Sala CPD, según se explica en el punto 4.6.1. Se realizarán dos capturas entre las 15:00 y las 23:00, en los turnos de tarde de los días laborables.

Finalizar el servicio realizando el parte del turno y dando las novedades si las hubiese al vigilante entrante.

2.4. Turno de noches

Al comienzo del turno se realizará una ronda a las dependencias de Monasterio de Irache 22 ***(antes se habrá dejado cerrada con llave la pta. de la calle de C/ Orcoyen)***, comprobando que estén apagadas todas las luces, bajadas las persianas y que no haya alguna fuga de agua en los baños (esta ronda se realiza al principio pero no siempre a la misma hora ya que hay un margen prudencial por seguridad).
Se sacará un listado con las visitas del día anterior de la base de datos y se enviará por correo electrónico al responsable de seguridad y se guardará en la unidad de red del Departamento. Para más información mirar Guía usuario gestión Autorizaciones.

Control de la temperatura de la Sala CPD, según se explica en el punto 4.6.1. Se realizarán dos capturas entre las 23:00 y las 07:00, en los turnos de noche de los días laborables y tres capturas entre las 19:00 y las 07:00, en los turnos de noche de los festivos y fines de semana.

Se abrirá la persiana de Monasterio de Irache a la primera persona que llega,* a partir de las 6:30 de la mañana, *comprobando su identificación.

Se finaliza el servicio realizando el parte del turno y dando las novedades si las hubiese al vigilante entrante.

3. FUNCIONES

3.1. Control de Acceso al Centro Informático

El control del acceso físico a los locales donde se encuentran ubicados datos de carácter personal es un punto esencial a tener en cuenta para evitar el acceso de personal no autorizado a dichos datos o los sistemas que lo gestionan.

En este sentido, se dispone de unas políticas, normas y procedimientos que evitan el acceso no autorizado a los locales donde se encuentran situados los sistemas de información con datos de carácter personal.

Al edificio del Centro de Informática (C/ Orcoyen, S/N) ***se debe acceder por la única puerta existente para tal fin y es preciso estar autorizado en el sistema de control de accesos del mismo.*** La puerta en cuestión está custodiada por un vigilante de seguridad armado en servicio de 24 horas diarias la totalidad de los días del año que suministra las tarjetas magnéticas necesarias e imprescindibles para dicho acceso.

Quedan registradas tanto la entrada como la salida del edificio de cualquier persona que acceda al mismo, así como el paso por determinadas puertas internas.

A la sala de servidores ubicada en el edificio del Centro de Informática ***solo tienen acceso parte del personal de NASERTIC y del Servicio de Infraestructuras Tecnológicas y Centro de Soporte, así como determinadas personas de empresas externas subcontratadas*** que necesitan acceder presencialmente a dicha sala debido a

su trabajo. Todos ellos han sido previamente autorizados por los responsables de dichas Unidades Administrativas.

Es decir, todo el personal citado tiene el acceso permitido al edificio a través de sus tarjetas magnéticas de identificación personal como centro de trabajo, pero ***solo unos pocos de ellos y debido a las responsabilidades de sus respectivas funciones tienen permitido el acceso a la sala de servidores.*** El resto de personas deberán acceder a través de la correspondiente tarjeta magnética suministrada por el vigilante de seguridad, que les será entregada a la entrada y recogida a la salida.

Existen dos tipos de Accesos:

Acceso Permanente:

Todas las personas que dispongan de una tarjeta personalizada de NASERTIC así como los miembros del Centro de Atención al Usuario (CAU) y de la Unidad de Vigilancia que posean también tarjetas personales.

Acceso Ocasional:

Las personas que deban tener acceso ocasional (normalmente a terceros) al Centro Informático, por el motivo que sea, deben estar dadas de alta en la aplicación Gestión de Autorizaciones para que se les asigne una tarjeta a su llegada dependiendo del nivel de acceso necesario. Así mismo dicha tarjeta deberá ser devuelta a su salida al vigilante.

Para que una persona esté dada de alta en la aplicación debe haber sido autorizada.

Solamente pueden autorizar los accesos al edificio 8 personas:

SECCIÓN	CARGO
DGITIP	Director Servicio Infraestructuras Tecnológicas y Centro de Soporte
	Jefe Sección de Infraestructuras Tecnológicas
	Jefe Sección de Producción
	Jefe Sección de Seguridad y Gestión de Rendimiento
NASERTIC	Director División de Servicios y Sistemas de Información
	Jefe Área Producción
	Jefe Área de Telco y Soporte
	Responsable de Seguridad
	Gerente

Puede estar autorizado de tres formas distintas:

1. Por estar dado de alta en las listas de las aplicaciones de “Gestión de Autorizaciones” o “Control de Accesos”.
2. Por estar autorizado a través de un correo electrónico concreto enviado (accesos@nasertic.es) con la suficiente antelación por una de las 8 personas que pueden autorizar accesos (el cual deberá ser guardado en la carpeta correspondiente del buzón de correo que estime oportuno el vigilante), con toda la información necesaria.

    - Empresa que va a realizar el trabajo
    - Persona(s) física(s) que va(n) a acceder al edificio (apellidos, nombre y N.I.F.)
    - Fecha y hora de la actuación
    - Motivo
    - Lugar de acceso (en qué sala va a tener lugar la actuación)
    - Tiempo estimado de la intervención
    - Indicación de si implica una interrupción de algún servicio

3. Por estar autorizado telefónicamente por una de las 8 personas que pueden autorizar accesos, solo en el caso de imponderantes o urgencias que impidan el envío del correspondiente correo electrónico.

Para un mejor seguimiento en cuanto a ***registros ISO 27001*** se refiere, es preciso que en la columna “Motivo” del Parte diario de Control de Accesos se especifique en los casos 2 y 3 la modalidad de la autorización y la persona autorizante (Ej. < Apellidos, Nombre persona que autoriza> < Tipo autorización (Telefónica o email) >). De igual forma, hay que anotar en la misma columna la persona a la que se avisa cuando la persona que entra no puede acceder si no es acompañada.

Los teléfonos de contacto de las 8 personas se encuentran en el Punto 7 Anexo 4 de la guía de Seguridad y orden en el CPD (Apartado de Responsables de autorización de acceso a las instalaciones)

Si una persona que intenta acceder al edificio no tiene autorizado su acceso a través de alguna de las tres formas definidas, el Vigilante de Seguridad se comunicará

telefónicamente con la persona más indicada, según el caso en cuestión, de las ocho citadas anteriormente. En última instancia intentará por todos los medios conseguir la autorización de acceso a través de cualquiera de los otros siete. Si el acceso debe llevarse a cabo y alguien se ha olvidado de notificarlo, se deberá evitar que la persona que intenta acceder se vaya sin conseguirlo, obteniéndolo en última instancia del Coordinador de Seguridad.

Así mismo se registrará en la Aplicación el nombre, apellidos y número del Documento Nacional de Identidad o documento equivalente de la persona y la empresa a la que pertenece.

Para la gestión de la aplicación dirigirse a la Guía usuario de Gestión de Autorizaciones.

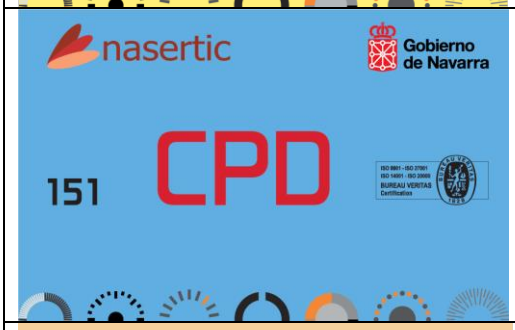
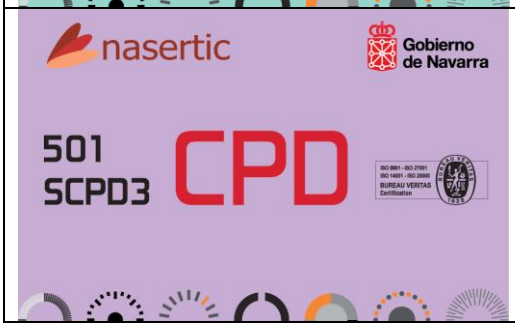
NOTA: Para cualquier petición de acceso que llegue al buzón de correo electrónico de la Unidad de Vigilancia y su remitente no sea ninguna de las personas autorizantes, se debe conseguir la autorización pertinente antes de que llegue el momento del acceso.

Hay dos tipos de Tarjetas:

Tarjeta personalizada.

Tarjeta de visita.

TARJETA	DESCRIPCION
	Tarjeta personalizada: se usa en cualquiera de las sedes y CBRS. Permite el acceso correspondiente en base a las autorizaciones precisas.
	Tarjeta personalizada: se usa en cualquiera de las sedes y CBRS. Permite el acceso correspondiente en base a las autorizaciones precisas.

TARJETA	DESCRIPCION
	Tarjeta de Visita Amarilla: solamente se usa en la sede Orcoyen a través del vigilante de seguridad. Permite el acceso al edificio por la puerta principal.
	Tarjeta de Visita Azul: solamente se usa en la sede Orcoyen a través del vigilante de seguridad. Permite el acceso al edificio por la puerta principal y al CPD.
	Tarjeta de Visita Servicios CPD1: solamente se usa en la sede Orcoyen a través del vigilante de seguridad. Permite el acceso al edificio por la puerta principal y al CPD a los clientes de Servicios CPD1.
	Tarjeta de Visita Servicios CPD2: solamente se usa en la sede Orcoyen a través del vigilante de seguridad. Permite el acceso al edificio por la puerta principal y al CPD a los clientes de Servicios CPD2.
	Tarjeta de Visita Servicios CPD3: solamente se usa en la sede Orcoyen a través del vigilante de seguridad. Permite el acceso al edificio por la puerta principal y al CPD a los clientes de Servicios CPD3.

TARJETA	DESCRIPCION
	Tarjeta de Visita CBRS: se usa en el CBRS a través del vigilante de seguridad. Permite el acceso al CBRS.

Periódicamente el responsable de Seguridad de NASERTIC es el encargado de solicitar la renovación de las tarjetas defectuosas o extraviadas, para ello solicita el nº de las tarjetas estropeadas a vigilantes.

NOTA: *Importante: notificar al responsable de Seguridad cualquier extravío de tarjeta para que proceda a su anulación.*

Se llevará el control del tarjetero de visitas *dejando constancia en el parte de servicio si se verifica la perdida de alguna y cualquier modificación realizada en sus accesos.*
Se anotará también**,** en el parte de servicio, ***las tarjetas que sean proporcionadas al personal que trabaje en el centro y cuando son devueltas.***

3.1.1 Área de Carga y descarga

Con objeto de evitar los riesgos derivados de las operaciones de carga y descarga y de mantener controlados los accesos a las áreas seguras motivados por operaciones de carga y descarga, la otra posibilidad de acceso al edificio del Centro de Informática, la otra puerta del edificio la de la puerta de carga y descarga, está provista de una barras antipático de salida al exterior (también es la salida de emergencia), una alarma antiapertura no deseada y una cámara de video vigilancia.

Para asegurar que sólo las personas autorizadas acceden al interior a través de la citada puerta permitiendo el acceso sólo a las áreas que sea necesario para llevar a cabo con éxito la operación de carga y descarga, sólo el vigilante de seguridad puede desconectar la alarma. Debe asegurarse de que hay una persona dentro del edificio controlando la operación de carga o descarga.

La persona indicada para supervisar la operación se encargará de inspeccionar el material para verificar que es el esperado y que no existe ningún riesgo inesperado derivado de su recepción o instalación. Cuando acaben los trabajos de carga o descarga, el vigilante de seguridad volverá a conectar la alarma.

Las persianas del montacargas deberán quedar en todo momento bajadas cuando no sean utilizadas. Todas las personas que lo utilicen serán las encargadas de llevarlo a cabo y el vigilante deberá observar que así sea.
Para más información mirar Guía seguridad y orden en el CPD.

3.1.2 Control de acceso de visitas a la sala de servidores

No es una práctica normal ***la realización de visitas a las dependencias del edificio del Centro de Informática*** y mucho menos a la sala de servidores del mismo, pero si esporádicamente es necesario el acceso de visitantes, ***a todos ellos se les aplicarán las normas de acceso e imprescindiblemente deberán realizar la visita acompañados de un funcionario de la Administración Foral "previamente autorizado por una persona responsable del Centro".***

La actuación en días festivos será la de hacer uso de algunos de los tfnos móviles de la dirección del centro (toda visita tiene que estar autorizada).

3.1.3 Acceso a los almacenamientos externos

Para intentar cumplir la normativa de seguridad vigente, algunas de las copias de seguridad de datos informáticos del Centro de Informática se realizan por duplicado, quedándose una de las copias en el lugar y su duplicado en un armario ignífugo ubicado en otro edificio, de tal manera que, si ocurriese un accidente que impidiera la utilización de uno de los juegos de copias, siempre quedaría el otro.

Para acceder dicho edificio externo, hay que pasar un control de acceso electrónico usando una tarjeta magnética a la que previamente se le ha tenido que dar autorización por parte del personal encargado de controlar el acceso a dicho edificio.

Solamente seis personas, que son las encargadas del transporte de los soportes magnéticos, ***tienen autorizado el acceso actualmente,*** aunque en su momento se elaboró una lista de personas que en condiciones extremas, solicitando el permiso de

acceso al personal encargado de su autorización y ante la ausencia de las siete personas que se encargan del transporte normalmente, podrían acceder al sitio físico en concreto.

3.1.4 Controles de seguimiento

Durante los turno de mañanas y noches el personal de seguridad imprimirá y enviará en formato electrónico la relación de accesos y los partes de incidencias cumplimentados por ellos mismos o por alguno de sus compañeros/as al responsable de Seguridad de NASERTIC, que los revisa y realiza acciones al respecto si procede.

Para sacar el listado del día seguir los pasos descritos en la ***Guía usuario gestión autorizaciones y custodia 3.5 Listado Control Accesos*** y siempre a la hora más próxima de las 7 de la mañana.

nasertic
División de Servicios Informáticos

Servicio de Seguridad. Control Acceso.

miércoles 19 de septiembre de 20

DNI	Nombre y Apellidos	Entrada	Salida	Tarjeta	Empresa	Motivo	Usuario
		08:04:49	09:00:48	00000167		Entrega 2 discos duros para sr. Garnika, visita oficinas.	
		08:10:07	08:26:34	00000111		Visita sr. J. Navarro. NAVARRO MARTINEZ JESUS A. TELEFONICA	
		08:15:35	09:25:46	00000168		CPD (rec. 2 discos duros del sr. Yanguas).	
		08:44:02	13:44:14	00000169		Visita sr. P. Ruiz (regresa en 5m).	
		09:01:27	09:04:14	00000112		Rec. paquetería, sr. Aldaz.	
		09:44:24	09:49:30	00000170		Salida: 09:44h. Olvidó su tarjeta arriba.	
		10:06:22	10:06:50	00000113		Entregar material oficina, sra. Larrea.	
		10:21:04	10:21:32	00000171		CAU, Copias de Seguridad.	
		10:44:11	11:08:12	00000172		CPD.	
		10:44:15	11:08:19	00000173		CPD. ZARIQUIEGUI ALDAVE EDUARDO EMAIL	
		10:44:19	11:08:24	00000174		CPD. ZARIQUIEGUI ALDAVE EDUARDO EMAIL	
		10:44:20	11:08:37	00000175		CPD. ZARIQUIEGUI ALDAVE EDUARDO EMAIL	
		12:44:37	12:45:25	00000114		Rec. listados (rec. aviso sr. Saragüeta).	
		13:55:07	16:05:52	00000169		Trabajo.	
		14:02:36	14:11:36	00000115		Visita vigilante.	
		17:05:10	19:13:35	00000176		TRABAJO CAU RUIZ LABATA JOSE SANTIAGO TELEFONICA	

Parte Vigilante 20/09/2012 2:33:57 Page 1 of 2

3.1.5 Procedimiento de actuación para los Sábados, Domingos y Festivos

Cualquier usuario de Hospitales que llame al Centro de Informática solicitando la asistencia de algún operador ***se le proporcionará el teléfono del Centro de Atención al Usuario del Gobierno de Navarra (CAU) 8484 25555.*** Será el CAU quien posteriormente contacte con Operación.

3.1.6 Acceso de personas no autorizadas

Ante la llegada de visitas que no estén autorizadas, hacer uso de algunos de los tfnos. móviles de la dirección del centro. ***Procurando no ser excesivamente rígidos*** así se evitaran dos fallos:

1º Denegar el acceso a una persona que debe realizar un trabajo in situ.
2º Despistes de conocimiento de alguna autorización de acceso que se traspapele.

- Se localizará a responsable de Seguridad, o de la DGIT.
- Preguntar quién les envía con el fin de localizar a alguien para su autorización.

3.1.7 Personal de SEGURIDAD (Vigilantes)

Por razones lógicas y de seguridad del edificio los accesos restringidos de visitas también afectan al personal de seguridad (en días laborales y festivos). ***No se pueden recibir visitas particulares, máxime si no quedan registrados en ningún sitio sus datos.***

Cuando un vigilante deje de prestar sus servicios en NASERTIC deberá devolver al responsable de seguridad las llaves y tarjetas que disponía para realizar sus funciones.

3.2. Control de Listados, Correspondencia y Paquetería

3.2.1 Listados (entrega, recogida)

Cuando vengan a recoger o llevarse listados, cajas, etc., se seguirá la siguiente secuencia de avisos. ***Primero avisaremos al personal de la unidad de Operación*** de turno. Si no los localizamos, avisaremos al personal de la Unidad de Impresión o Unidad de Seguridad. Si tampoco los localizamos, avisaremos al responsable del Área de

Producción. ***Si tampoco lo localizamos, avisaremos a la unidad de Mantenimiento y, como último caso, a la Unidad de Administración.***

3.2.2 Control de Correspondencia

Deben de provocar sospecha:

- Remitente desconocido, no habitual o no escrito.
- Cierto grosor.
- Contenido rígido.
- Peso desproporcionado.
- Distribución desequilibrada.
- Manchas u olores extraños.
- Exceso de franqueo.
- Matasellos y remitente de lugares diferentes.
- Dirección con errores, incompleta o excesiva.
- Falta de ortografía.
- Anotaciones como “PERSONAL”, “CONFIDENCIAL”, ETC.

Se verificarán las Cartas declaradas como sospechosas del siguiente modo:

- COMPROBANDO SI EL REMITENTE HA REALIZADO EL ENVIO.
- COMPROBANDO SI EL DESTINATARIO ESPERA DICHO ENVIO.

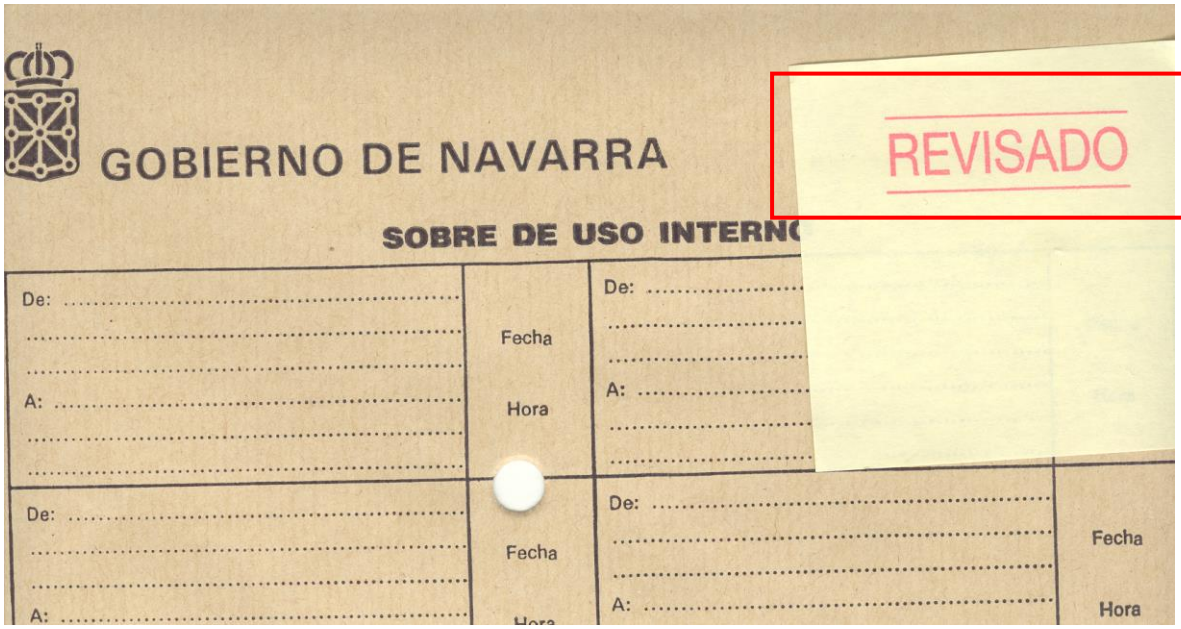
Cuando desaparezcan las dudas:

- Se estampara un sello de ***REVISADO*** en:

    - Ambas caras de la carta.
    - En varias caras de los paquetes, incluida la principal.

Si la correspondencia ha sido traída de Monasterio de Irache, deberemos seguir el mismo procedimiento, salvo que sea un sobre de correspondencia interna del Gobierno de Navarra. En este caso pondremos el sello revisado en un post-it y lo pegaremos al sobre.

Después se entregará la correspondencia.



3.2.3 Entrega de paquetes no certificados

Todos los paquetes deben tener un responsable del paquete que podrá ser de NASERTIC o de la DGIT.

Se deberá contactar con el destinatario del paquete para seguir sus indicaciones. De no existir destinatario se contactará con el responsable del mantenimiento para seguir sus indicaciones.

La persona que trae el paquete ***no debe dejarlo nunca en la entrada principal***. Lo tiene que introducir en el centro él mismo y no el personal de seguridad (con el fin de unificar criterios y evitar situaciones discordantes con las personas de las empresas de Transportes).

De ordinario ***se contactará con la persona encargada del mantenimiento ante cualquier tema de entrega o recogida de papel (Papelera del Arga, Papel Diez, etc.),*** exceptuando la gestión de los listados diarios. También se contactará con él si vienen a entregar ***material de limpieza***,

3.2.4 Entrega de paquetes o cartas certificadas

- Si la carta o paquete certificado vienen a nombre de Nasertic, el vigilante que esté de turno lo recogerá él mismo y llamará a la Unidad de Administración para dar el aviso.

Firmará con nombre, apellidos y DNI, por ser el protocolo de recogida de Correos. El nº de TIP es opcional, pero siempre deberá estar acompañado del número de DNI.

- Si la carta o paquete certificado viene a nombre personal de un trabajador de Nasertic, el vigilante llamará a dicha persona para que haga la recogida personalmente. En caso de ausencia de la misma, el vigilante se pondrá en contacto con la Unidad de Administración para que se encargue de la recogida.

3.3. Gestión de custodia

Los vigilantes disponen de unos lugares habilitados para la custodia de llaves, portátiles que usa NASERTIC para realizar sus guardias,…

3.3.1 Control de llaves (entrega y recogida)

Cuando alguien necesita una llave la solicita a los vigilantes, ellos miran ***si la persona está autorizada a coger esa llave, si es así, se la dan y apuntan en el parte diario la hora de entrega y devolución y en la aplicación diseñada para tal fin(Gestión Prestamos).***

- ***Cuando personal de cualquier empresa externa*** al centro ***las soliciten, especialmente si se trata de los Cuadros de Baja Tensión o las llaves de comunicaciones*** (exceptuando las llaves de limpieza al personal de la Empresa Externa de Limpieza), ***se deberá notificar al encargado de Mantenimiento.***

Hay dos ***llaves de Justicia*** que ***solo se deben entregar a los responsables de Seguridad, Administración y Mantenimiento así como a los Operadores***. ***Apuntar en el Parte de Servicios las horas de entrega/devolución de las llaves y quién las solicita/devuelve*** (consta en el protocolo de actuación la relación de personas autorizadas y su gestión fuera del horario laboral).

Actualmente ya esta operativa la aplicación para la ***Gestión Prestamos***.

3.3.2 Ordenadores portátiles

Apuntar en el Parte de Servicios las ***horas de recogida/devolución así cómo el nombre de quién lo solicita/devuelve y en también se registrara en la aplicación de Gestión Prestamos***. Solo pueden solicitarlos las personas de Unidad de Operación

También hay un portátil en custodia portátil para las guardias de comunicaciones de IRACHE, si se presta ese portátil deberemos proceder como con los de Operación.

3.3.3 Sobres de usuarios de emergencia y protocolo de actuación

Existen tres sobres de Usuarios de Emergencias junto con unas normas de actuación precisas, donde constan las personas que los pueden solicitar.
El personal nuevo de vigilancia que no conozca quiénes pueden solicitarlos ***deberá contrastar sus datos en la aplicación Gestión de Prestamos.***

3.3.4 Custodia del Botiquín del Centro

La Unidad de Vigilancia es la encargada de la custodia del botiquín que el centro dispone.

La unidad de Vigilancia también es la encargada de facilitar el acceso al contenido del botiquín que se encuentra en su interior.

Si se observa que algún componente del botiquín está próximo a su caducidad o agotar su existencia se notificará al Responsable de mantenimiento mediante un correo electrónico.

3.4. Correo electrónico

Para poder desarrollar sus funciones los vigilantes disponen una cuenta de correo electrónico, de la que son responsables de su gestión y del buen uso.

La cuenta de correo es: accesos@nasertic.es.

Para su buen uso deben leer la Guía Seguimiento Correo Electrónico.

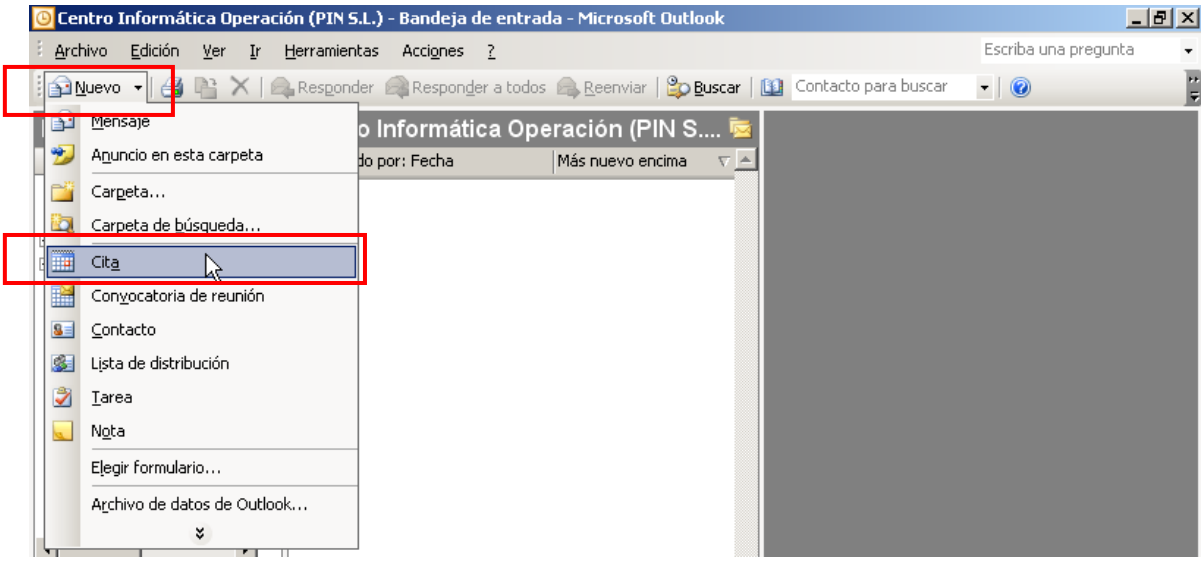
No se borrará ninguno de los mensajes que se reciban.
Una copia de los correos electrónicos que llegan al buzón de los vigilantes llega al coordinador de la Seguridad del Centro.

NOTA: ***Precaución ante la recepción de virus. No abrir ningún correo cuyo remitente sea desconocido. Si se sabe que un mensaje contiene virus eliminarlo de la bandeja de entrada y también de elementos eliminados, sin llegar a abrirlo.***

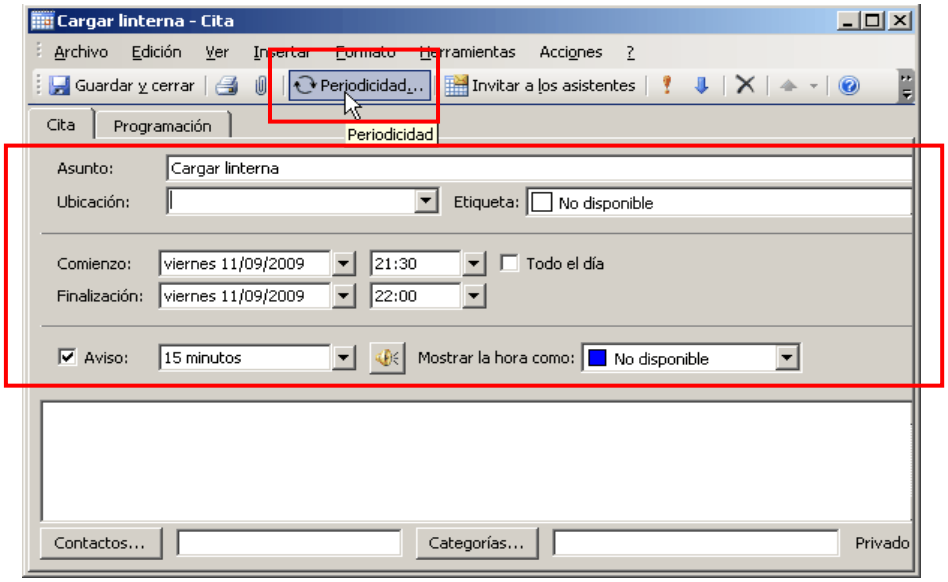
3.4.1 Creación de un aviso en el correo electrónico

Si por necesidad necesitamos crear un aviso nuevo en el correo electrónico deberemos seguir las siguientes instrucciones:

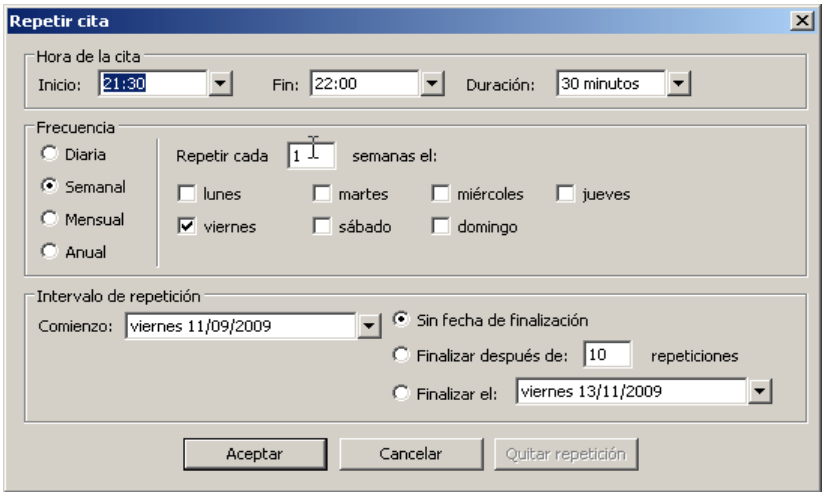
1. Iremos al icono ***nuevo*** y desplegaremos el menú contextual y seleccionaremos ***Cita.***



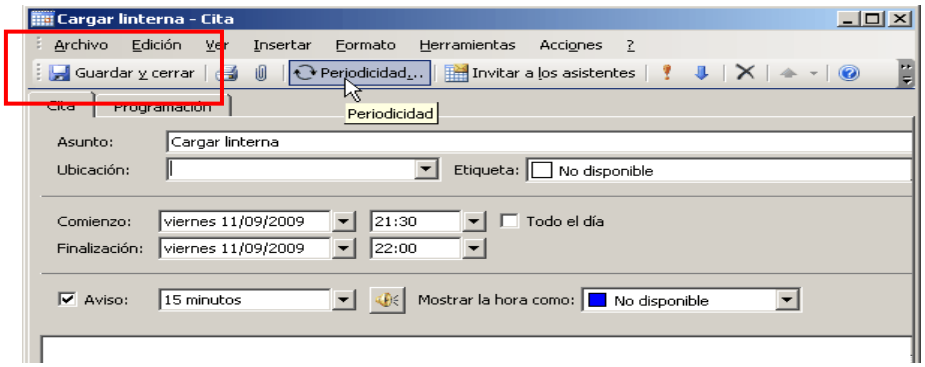
2. Rellenaremos la información que creemos oportuna y después pulsaremos el botón ***Periodicidad.***



3. Ahora le diremos la periodicidad que deseamos para el aviso y después pulsaremos el botón ***Aceptar.***



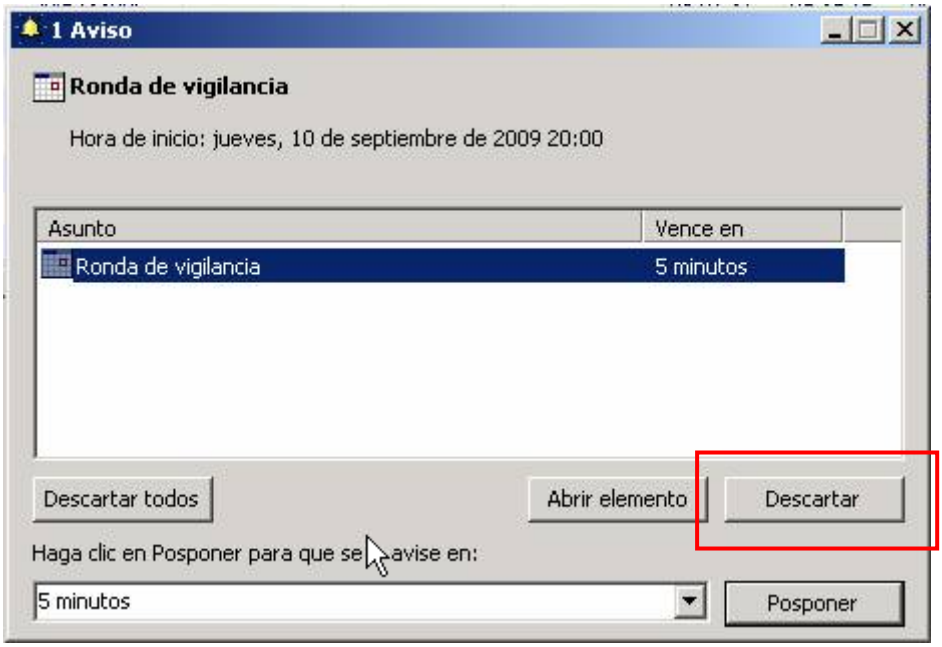
4. Finalmente pulsaremos el botón Guardar y cerrar en la ventana de la cita.



3.4.2 Avisos en el correo electrónicos

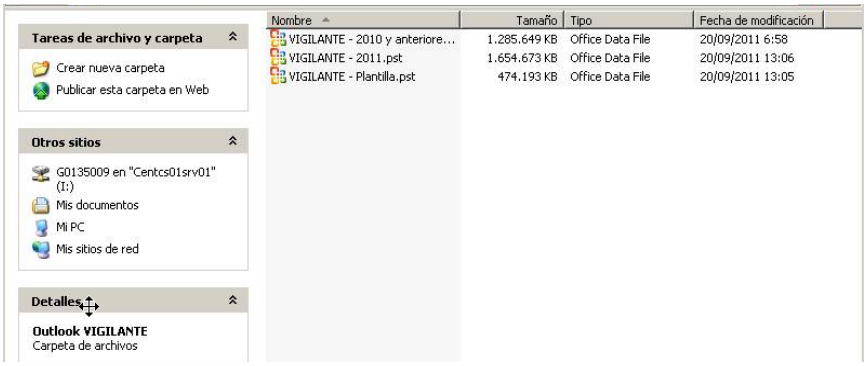
Para recordarnos que se deben realizar ciertas acciones (como por ejemplo la ronda del edificio) nos saldrá con cinco minutos de antelación a la hora establecida una ventana emergente recordándonos la acción a realizar.

Deberemos pulsar el botón ***DESCARTAR***, de esta forma ya no volverá a salir hasta la próxima vez que esté programada la acción a realizar.

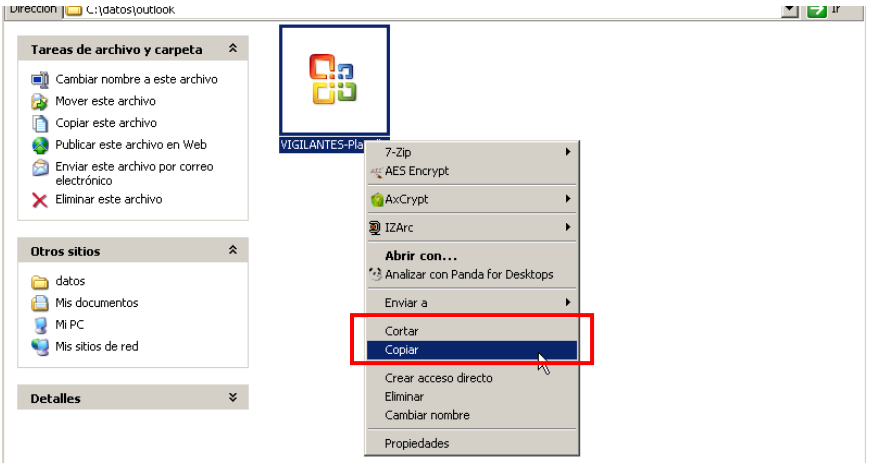


3.4.3 Crear Archivo de Carpetas Personales (PST)

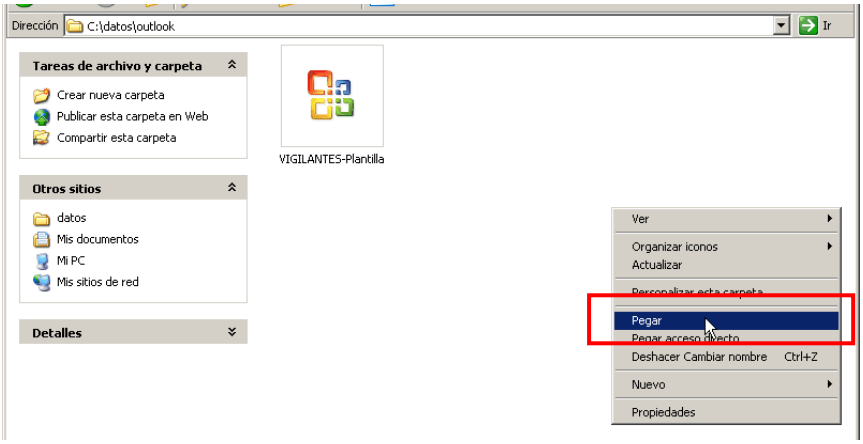
El primer día del año deberemos ir a la unidad de Red de Vigilancia y hacer una copia del archivo VIGILANTES – Plantilla.pst



1. Para ello deberemos seleccionar el archivo VIGILANTE –Plantilla y pulsar el botón derecho del ratón y seleccionar la opción copiar que nos aparece.

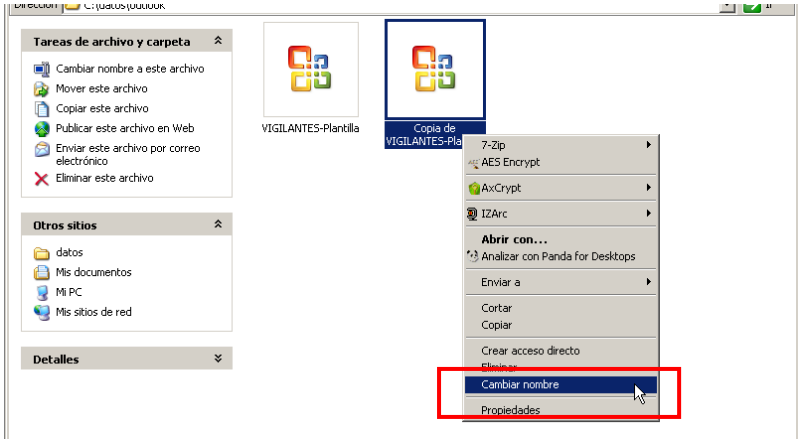


2. Ahora deberemos seleccionar cualquier zona para que ya no este seleccionado el archivo (deje de estar en azul) y volvemos a pulsar el botón derecho del ratón y esta vez seleccionamos la opción ***pegar***



3. Ahora tendremos una copia de la plantilla a la cual debemos cambiarle el nombre por:

   VIGILANTE – XXXX siendo XXXX el año que se empieza.



Ahora deberíamos agregarla al Outlook

3.4.4 Agregar Archivo de Carpetas Personales (PST)

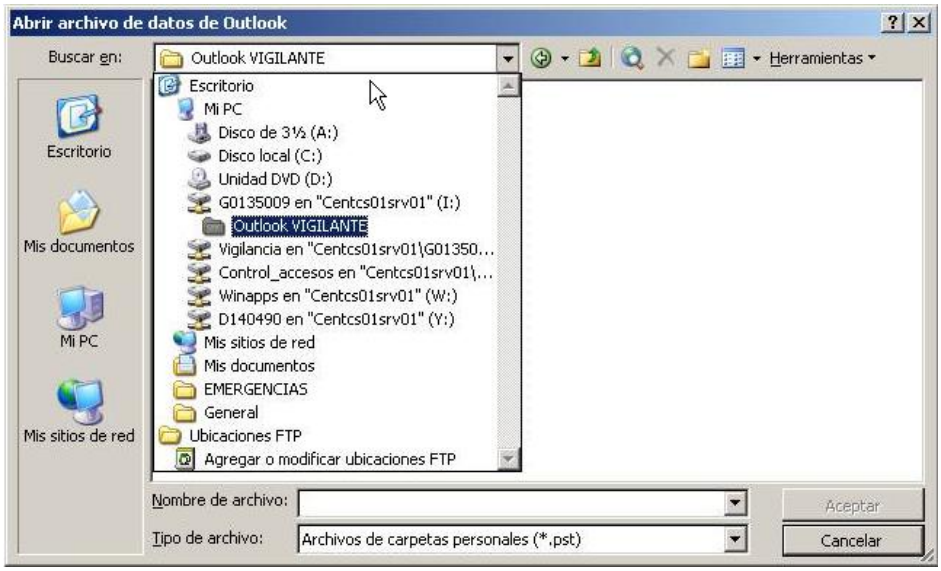
El primer día laborable de cada año deberemos agregar un PST (Carpetas Personales) nuevo para el año que empieza.

Los pasos que se deben seguir para agregarlo son los siguientes:

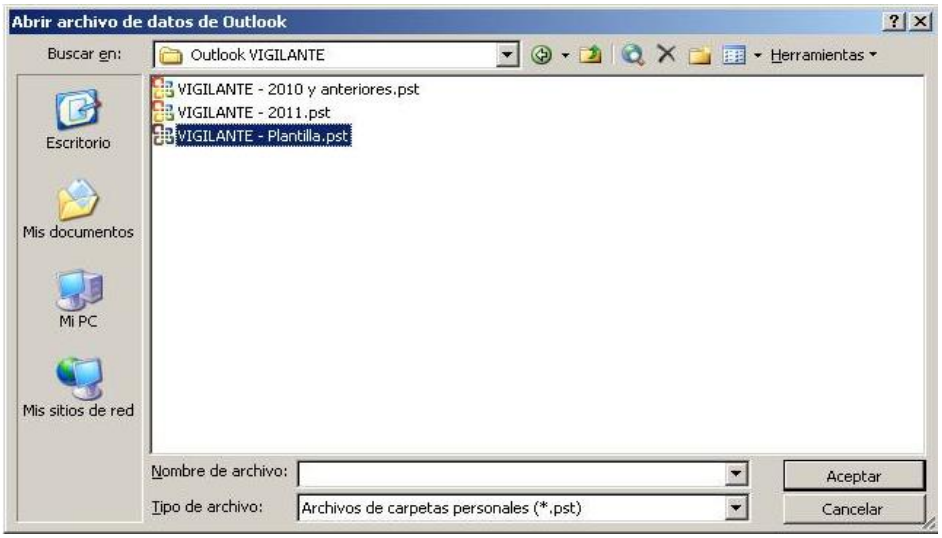
1. Desde el menú superior de la aplicación del correo electrónico deberemos seleccionar la opción ***Archivo → Abrir → Archivo de datos de Outlook***



2. A continuación deberemos seleccionar la ruta donde se encuentra el PST del año que empieza



3. Ahora seleccionaremos el nuevo PST creado y pulsaremos el botón Aceptar. Para ello deberemos seleccionar el archivo en cuestión.



3.5. Buen uso del PC

Cada Vigilante es responsable de que el ordenador se quede bloqueado cada vez que deban abandonar el puesto de trabajo.

3.6. Control del material de limpieza

3.6.1 Limpieza cristales

Cuando vengan de la empresa externa encargada de la limpieza de *los cristales,* ***si está el responsable de Mantenimiento se le avisará*** y sino ***se dejará una nota de los cristales que han limpiado*** para que el/la vigilante del día siguiente se lo notifique. Se ***deberá firmar el parte de trabajo de la empresa (si lo presentan) poniendo por orden (P.O.).*** Cuando vengan a limpiar los cristales exteriores se firmará igualmente. Al día siguiente ya verificará el responsable de mantenimiento si los han limpiado.

3.6.2 Cajas depositadas en la sala CPD

Cuando entren materiales a la Sala CPD, ***el personal de seguridad es responsable de que no quede ninguna caja y demás restos de embalaje*****;** invitará a las personas que han dejado dicho material a que los saquen del centro (para ello, en caso necesario, pueden utilizar la pta. de emergencia).

Si, por la razón que sea, los dejan para sacarlos otro día, que los depositen ***fuera de la Sala CPD en el pasillo***. Poner atención por ser material combustible.

Para más información mirar Guía seguridad y orden en el CPD.

3.7. Vídeo Vigilancia

El sistema de Video vigilancia efectúa automáticamente grabaciones de video por detección de movimiento de todas las cámaras.

En cada turno se realizará un control del sistema de video vigilancia para comprobar el correcto funcionamiento de la grabación y almacenamiento de los sistemas de CCTV.

Los ficheros de video se pueden consultar manejando el software del visor del sistema.

3.8. Gestión del reservado de vehículos

Disponible para el centro las 24 horas de todos los días del año, previa colocación OBLIGATORIA y en lugar visible dentro del vehículo de la tarjeta autorizadora expedida por el Ayuntamiento de Pamplona.

Está habilitado para la recepción y recogida de materiales. Preferentemente, que las empresas de mantenimiento que lo utilicen lo hagan para descargar sus herramientas y demás útiles… buscando después otra zona donde estacionar su vehículo.

Se actuará de forma flexible, según los casos.

En los supuestos en que personal de empresas externas realicen trabajos en el centro, deben comunicar al vigilante el uso del estacionamiento (estar atentos porque en ocasiones entran sin informan de ello y además, al salir del centro lo siguen ocupando mientras suben a Mº de Irache).

Cuando excepcionalmente sea necesario utilizarlo por personal del centro, será dejando una de las plazas libre y trasladando el vehículo en cuanto sea posible a otro estacionamiento.

En la unidad de red del departamento se dispone de diferentes informes sobre el tema (Actuación ante vehículos no autorizados, aviso a Grúa, anotaciones de matrículas,….)


Ayuntamiento de Pamplona
Iruñeko Udala

Area de Seguridad Ciudadana
Policía Municipal
Jefatura

899

Se autoriza al vehículo: PORTADOR DE ESTA TARJETA

Al servicio de:

A ACCEDER Y ESTACIONAR EN EL RESERVADO DE LA C/ORCOYEN S/N FRENTE AL CENTRO DE INFORMATICA DE GOBIERNO DE NAVARRA

Pamplona, 23 de diciembre de 2008

EL JEFE DE POLICIA MUNICIPAL

P.O.

Ayuntamiento de Pamplona
Policia Municipal
Jefatura

Caduca el día:

31 de diciembre de 2009

3.9. Gestión de siniestros (averías) urgentes

La Unidad de vigilancia se encargara de gestionar los siniestros y las averías en los edificios de Nasertic: calle Orcoyen, San Jorge y laboratorio de Villava. De la siguiente forma:

- En horario laboral se encargara el personal de mantenimiento directamente.
- Fuera del horario laboral, cuando se produzca una incidencia urgente que no pueda esperar (p.ej. una fuga de agua), en alguno de los edificios, ***el personal de Nasertic se pondrá en contacto con la Unidad de vigilancia de calle Orcoyen***. Esta será la encargada de recoger los datos de la incidencia y ponerlos en conocimiento del personal correspondiente (técnico de mantenimiento o responsable de mantenimiento y seguridad) según los datos de que dispongan, vacaciones etc

La Unidad de Vigilancia tiene disponibles los números de teléfono de contacto y números de póliza de la correduría de seguros y del correspondiente seguro (por si los necesita usar o facilitar al técnico de mantenimiento o responsable de mantenimiento y seguridad) que comprende a todos los edificios de la empresa, aunque en el documento ponga que son de la sede de SAN JORGE son genéricos para cualquier Sede.

3.10. Informes y novedades

La información se podrá difundir mediante forma verbal o escrita.

VERBALES

La incidencias y, en especial las emergencias o alarmas, que ocurran durante el servicio se comunicarán, para que tengan conocimiento de lo sucedido y de las medidas que se han tomado:

- Al responsable de seguridad.
- El vigilante al inspector de servicios.

Se tendrá en cuenta que los informes o novedades que se den de forma verbal, se pasarán a escrito con la mayor brevedad posible, entregando el mencionado informe a las personas descritas en la parte superior.

Si en algún momento el informe se tuviera que entregar a los Cuerpos Policiales, antes se notificará al responsable de Seguridad del NASERTIC para su comprobación y verificación de los datos que se adjuntan.

ESCRITOS

Todos los comunicados de incidencias del servicio deben escribirse señalando con precisión:

- La hora en el que ha comenzado la incidencia.
- La hora en la que ha acabado.
- Todos los detalles de la incidencia.

Todos los documentos por escrito deberán ser rellenados en formato electrónico.

El que redacte un documento deberá fecharlo, identificarse mediante su nombre y apellidos y validarlo mediante su firma.

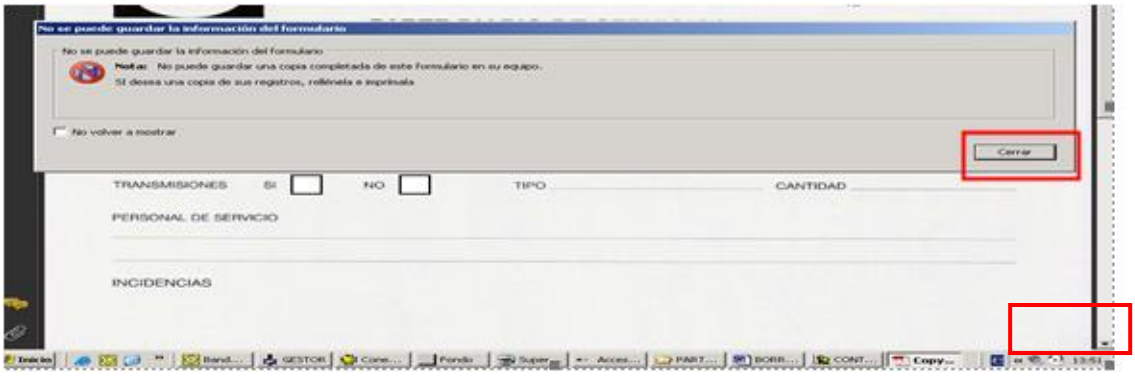
Existen dos tipos de Informes:

3.10.1 Informe Diario

En él se indicarán todas las incidencias sucedidas durante el turno (entrega de llaves, recogida de portátiles,….)

La plantilla del Informe Diario se encuentra en la unidad de red de vigilancia.

Clica en Cerrar

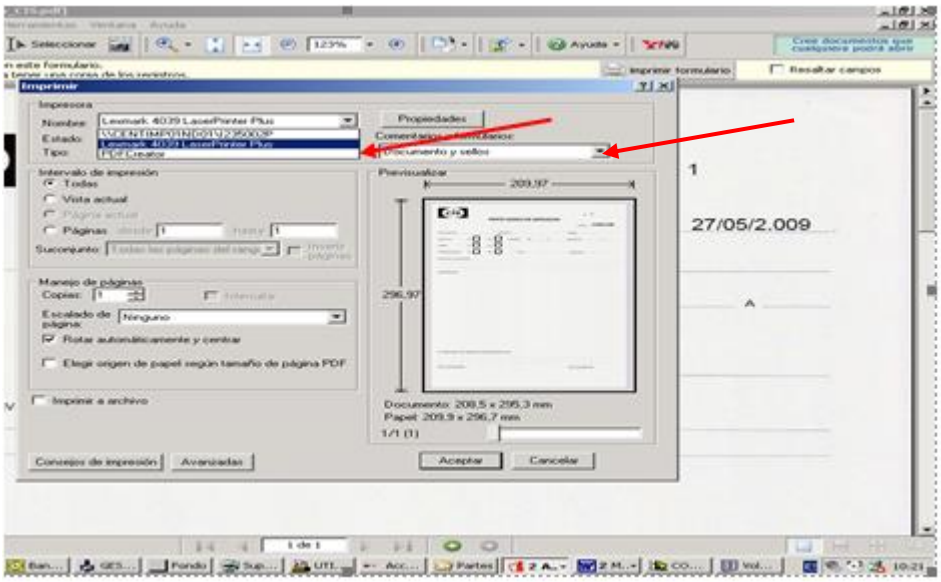


A continuación rellena los datos y escribe las incidencias del servicio.

Por **si *falla el ordenador y se cierra la aplicación o te ves obligado a cerrar la sesión por cualquier motivo, para evitar pérdidas de datos,*** copia lo que escribes y guárdalo en un documento Word.

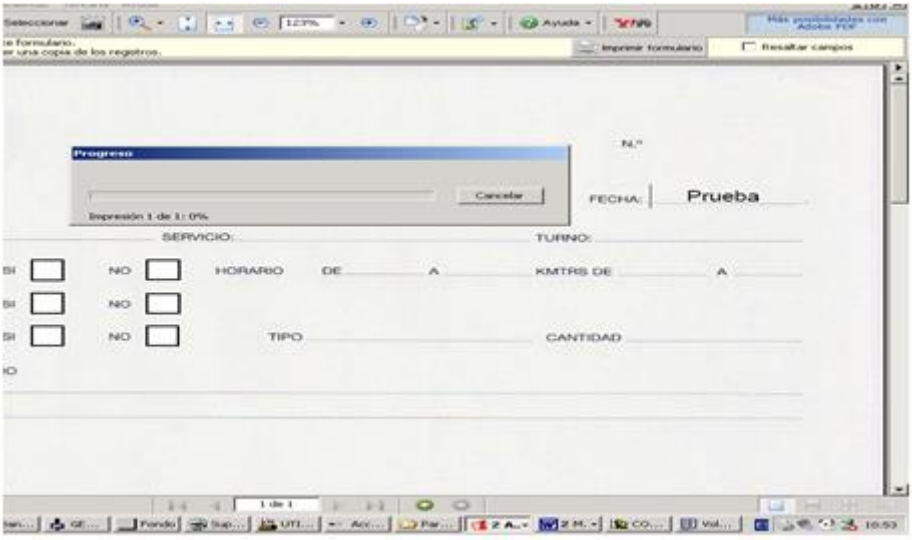
Finalizado el servicio, genera dos copias del Parte, una en papel físico y otra en un archivo PDF que se guardará en el ordenador. Para ello sigue estos pasos:

1. Clica en ***impresora*.**
2. *Desde esta flecha abre para elegir impresora.*
3. ***Imprime una copia física*** para la empresa de seguridad (impresora Lexmark). ***ACEPTAR.***
4. ***Imprime una copia digital*** seleccionando impresora virtual ***PDFCreator ACEPTAR.***

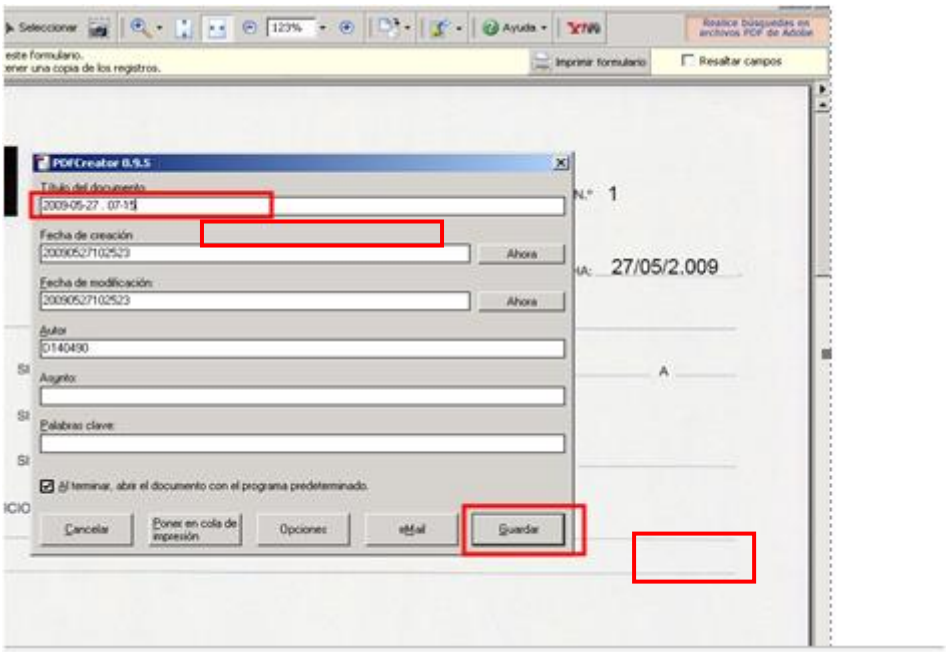


Clica en **Aceptar.**

*Y **espera unos segundos**…*

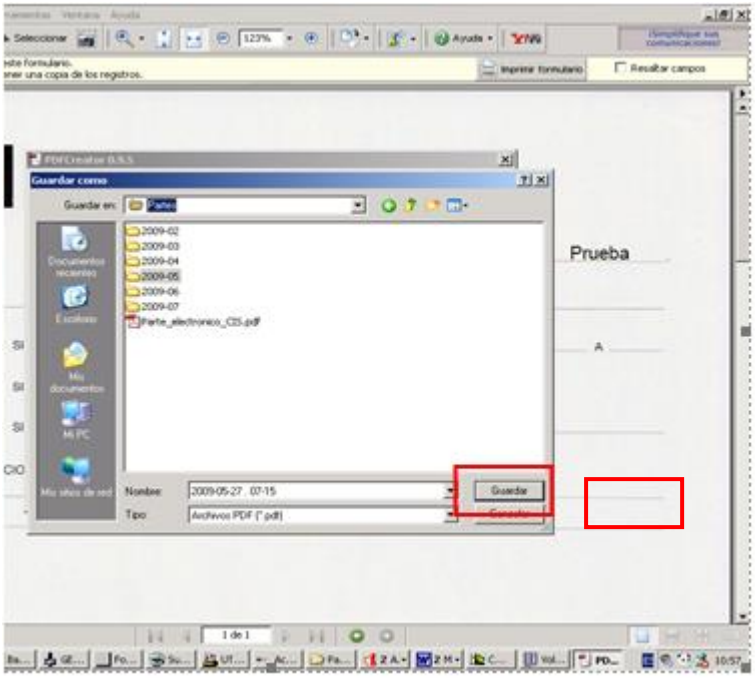


Pon título al documento con la fecha del día y turno de trabajo (***hacerlo todos igual****), por ejemplo* ***2009-05-27 . 07-15*** y ***Guardar*** (seguir el mismo orden: año, mes, día y horario AAAA-MM-DD . HE-HS).



Selecciona ***Guardar,*** *para grabarlo* ***en la carpeta que le corresponde***.

Vuelve a clicar en ***Guardar.***



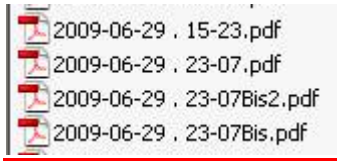
La aplicación nos indica que está guardándolo mientras nos muestre esta ventana.



Clica en **la X para salir.**

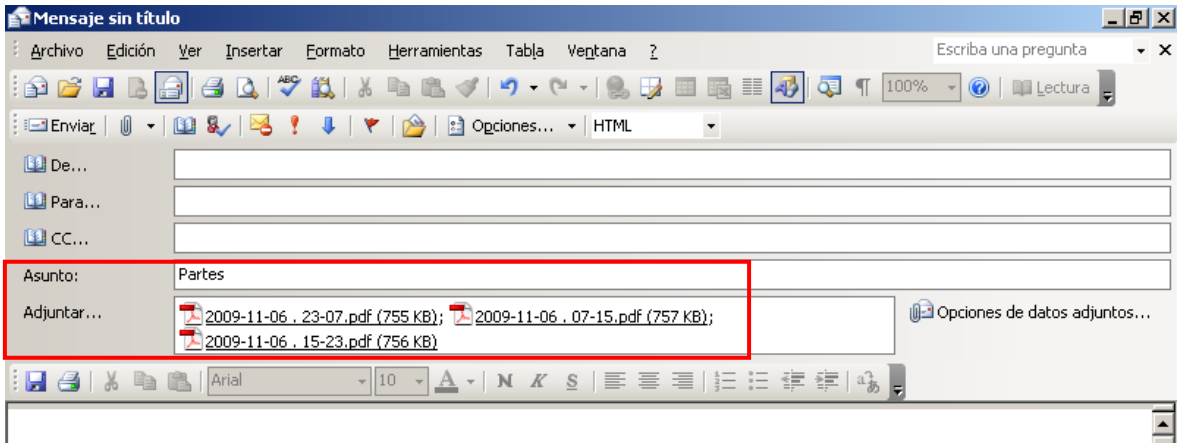
Por último cierra el documento.

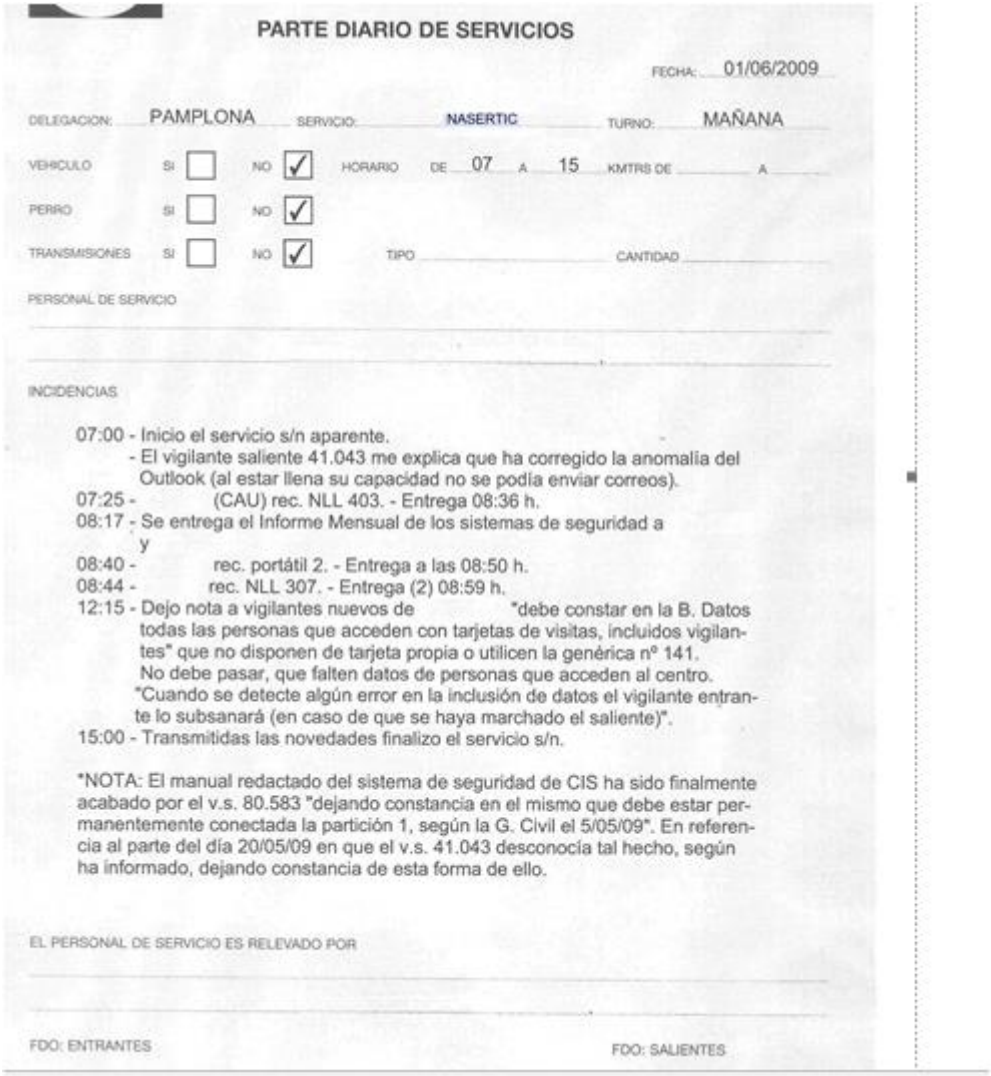
NOTA: Si tenéis necesidad de rellenar un parte largo, **guardar lo que exceda** de una hoja **en otro parte**. De lo contrario lo perderéis sin opción a recuperarlo. En este caso, la nomenclatura de los informes será la misma salvo que los siguientes informes deberán ir con un Bis (para la 2 hoja), Bis2 (para la tercera hoja) y así sucesivamente.



Abriremos el Parte digital para comprobar que se ha creado bien.

El Vigilante del turno de Mañanas se encargará de enviar un e-mail al responsable de seguridad y de mantenimiento adjuntando los partes del día anterior, poniendo en el Campo *Asunto*: ***Partes***.





PARTE DIARIO DE SERVICIOS

FECHA: 01/06/2009

DELEGACION: PAMPLONA SERVICIO: NASERTIC TURNO: MAÑANA

VEHICULO SI ☐ NO ☑ HORARIO DE 07 A 15 KMTRS DE ____ A ____

PERRO SI ☐ NO ☑

TRANSMISIONES SI ☐ NO ☑ TIPO ____ CANTIDAD ____

PERSONAL DE SERVICIO

INCIDENCIAS

07:00 - Inicio el servicio s/n aparente.
- El vigilante saliente 41.043 me explica que ha corregido la anomalía del Outlook (al estar llena su capacidad no se podía enviar correos).
07:25 - (CAU) rec. NLL 403. - Entrega 08:36 h.
08:17 - Se entrega el Informe Mensual de los sistemas de seguridad a y
08:40 - rec. portátil 2. - Entrega a las 08:50 h.
08:44 - rec. NLL 307. - Entrega (2) 08:59 h.
12:15 - Dejo nota a vigilantes nuevos de "debe constar en la B. Datos todas las personas que acceden con tarjetas de visitas, incluidos vigilantes" que no disponen de tarjeta propia o utilicen la genérica nº 141.
No debe pasar, que falten datos de personas que acceden al centro.
"Cuando se detecte algún error en la inclusión de datos el vigilante entrante lo subsanará (en caso de que se haya marchado el saliente)".
15:00 - Transmitidas las novedades finalizo el servicio s/n.

*NOTA: El manual redactado del sistema de seguridad de CIS ha sido finalmente acabado por el v.s. 80.583 "dejando constancia en el mismo que debe estar permanentemente conectada la partición 1, según la G. Civil el 5/05/09". En referencia al parte del día 20/05/09 en que el v.s. 41.043 desconocía tal hecho, según ha informado, dejando constancia de esta forma de ello.

EL PERSONAL DE SERVICIO ES RELEVADO POR

FDO: ENTRANTES FDO: SALIENTES

El parte impreso físicamente se FIRMARÁ y se colocará en la bandeja habilitada para la empresa externa de Seguridad.

NOTA: *Durante la primera semana de cada mes, el interlocutor de seguridad imprimirá, si no lo estuviesen ya, todos los partes de incidencias del mes vencido, ordenándolos cronológicamente en la carpeta establecida al efecto. Deberán estar firmados por todo el equipo de seguridad para su archivo.*

3.10.2 Informe Mensual de evaluación del estado de los sistemas de seguridad

Este informe se crea mensualmente, ***antes del día 10 de cada mes*** y en él se indica el estado del Sistema de Seguridad, así como las incidencias más reseñables del mes. Lo deberá realizar la Unidad de Vigilancia, lo guardará en la unidad de red y lo enviará al responsable del Área de Producción.

Las pautas que se deben seguir para redactar el Informe son las siguientes:

1. Al indicar las anomalías subsanadas, poner la ***SITUACIÓN ANTERIOR*** y la ***SITUACIÓN ACTUAL,*** pero sólo el mes en que se arregla la anomalía. En los siguientes informes mensuales no hace falta repetirlo.

NOTA: Antes de empezar a redactar el nuevo Informe hacer una copia del documento Word para tener los informes de todos los meses.

El Informe Mensual ***es un informe exclusivamente de NASERTIC-División Servicios Informáticos y para NASERTIC "NO DEBIENDO SER ENTREGADO A NINGUNA DE LAS EMPRESAS DE SEGURIDAD".*** Únicamente pondremos lo concerniente a NASERTIC (nada sobre los sistemas de la Empresa de Seguridad).

INFORME MENSUAL DE ENERO - 09
PIN, S. L.

ESTADO DE LOS SISTEMAS DE SEGURIDAD

SEGURIDAD CONTRA INCENDIOS

Extinción por agua nebulizada

- Uno de los manómetros de los cilindros de nitrógeno se encuentra en el *límite de bajada* establecido en los 180 bar.

Central de incendios

- Tras la formación de un cuarto en el interior de UPS ha quedado obsoleta la definición de esta zona en la Central *al no especificar a que zona corresponde cada cual* (líneas 5 y 6).

PLAN DE EMERGENCIA DE EVACUACIÓN

- **Seguimos desconociendo la existencia del mismo para este centro.**
- **Una parte del personal, relativamente nuevo, de este centro desconoce el recorrido a seguir de las Salidas de Emergencias**

ALUMBRADO DE EMERGENCIA Y SEÑALIZACIÓN

- Debido a trabajos realizados del A/A se ha desprendido *este pequeño*  *panel informativo de salida* en planta baja (pasillo técnico). El cual no ha quedado en muy buen estado.
- La Sala de Reuniones y el nuevo cuarto del interior de UPS carecen de *paneles informativos de salida.*

CENTRAL DE ALARMAS

- El monitor de la sala de producción (alarmas) *no refleja las alarmas* que se producen en el centro desde el cinco de abril de dos mil siete.
- Desde el quince de noviembre se viene observando en la consola de robo: *"estado de sistema no listo"*. Parece ser debido a **los sensores de la pta. principal, no están de forma simétrica.** *Ello puede crear cierta dificultad para saber si están todos los dispositivos de protección en activo.*

CONTROL DE LLAVES

- *Mayo 2008*: -El operario de mantenimiento recoge 3 llaves de Storagetek *(comunicando que **mandará al personal de Seguridad un email para que quede constancia del destino final de dicha llave)*.
- Con fecha 13/08/2008, se detecta la perdida de 3 llaves en el El último movimiento fue el día 11/08/2008 a las 11:22horas por la vigilante . Desde este día al día siguiente, en que se echan en falta para su utilización, los vigilantes que han pasado por el centro de trabajo han sido por este orden:

Estas llaves se colocaban en un lugar accesible y visible para su utilización diaria . Estas llaves correspondían a la
Ha quedado en conocimiento de la Policía Foral y estamos a expensas de la resolución que se tome al respecto.

- Con fecha 09 de Enero entrega a vigilantes 2 llaves del nuevo armario de llaves, ; y la otra es para nuestro uso.
  Con la misma fecha entregamos a 1 llave de la caja de copias.
- Con fecha 12 de Enero al tomar temperaturas en la sala del host encontramos el armario ignifugo abierto, no se puede cerrar porque están los anclajes de la puerta hacia afuera. Desde Navidad extravió la llave y vienen utilizando un duplicado. Con fecha de 13 de Enero se localiza dicha llave según informa mediante un email y comenta que han echo otra copia de dicha llave.

SISTEMAS DE CERRAMIENTOS

- Se observa que la pta. principal no abre bien se queda en ocasiones como enganchada.
- La puerta del Host en algunas ocasiones se encuentra la pta. abierta no habiendo nadie trabajando en la sala.

DETECTORES DE INTRUSIÓN

Elementos detección-sensores de seguridad

- Hay un volumétrico en UPS *pendiente de ser fijado a la pared* tras la remodelación realizada en esta estancia.

3.11. Notificación de Incidencias

Fuera de la jornada laboral, a la hora de notificar incidencias se tendrá en cuenta la gravedad de la misma para decidir si avisar a la dirección de NASERTIC, a la persona de mantenimiento y/o la empresa externa de Vigilancia.

Si fuera necesario, se seguirán las pautas de contacto con los cuerpos de Seguridad del Estado (Consultar documento confidencial custodiado por los vigilantes de seguridad).

4. GESTIÓN Y CONTROL DE SISTEMAS DE SEGURIDAD

4.1. Alarmas de Intrusión

Existen dos centrales de intrusión, conectadas a central receptora y en comunicación con el servicio de vigilancia de calle Orcoyen. Son las siguientes:

4.1.1 Alarma intrusión calle Orcoyen

La alarma de Intrusión del Centro de calle Orcoyen está compuesta por:

1	Central de alarmas supervisada.
1	Consola de display alfanumérico.
1	Consola virtual IP.
1	Sirenas interiores.
10	Detectores volumétricos.
12	Contactos magnéticos de apertura de puerta.
17	Detectores sísmicos.
3	Centrales de incendios supervisadas.

4.1.2 Alarma intrusión San Jorge

La alarma de Intrusión del Centro de San Jorge está compuesta por:

1	Central de alarmas supervisada.
1	Consola de display alfanumérico.
1	Consola virtual IP.
1	Sirenas interiores.
4	Detectores volumétricos.
1	Centrales de incendios supervisada.

Para su manejo iremos al Manual de esta alarma.

4.2. Alarmas del Sistema de Refrigeración

Para su manejo iremos a las Guías de Mantenimiento de esta alarma.

4.3. Alarmas de detección y extinción de Incendios

La alarma de detección y extinción de Incendios del Centro Informático está compuesta por:

Detección.

2	Central de detección de incendios CERBERUS CZ10/16.
98	Detectores iónicos en techo y suelo.
99	Detectores ópticos de humo.
1	Detector térmico.
112	Indicadores de acción.
3	Indicadores óptico-acústicos de halón disparado (actualmente anulados).
5	Bocinas de alarma.
7	Bocinas de pre-alarma.
24	Pulsadores de alarma.
3	Pulsadores de disparo halón (actualmente anulados).
6	Pulsadores de bloqueo halón (actualmente anulados).

Extinción.

1	Batería de agua nebulizada con 6 cilindros de H_2O y 2 cilindros de nitrógeno de 80 l.
4	Pulsadores de disparo manual.
2	Electroválvulas de disparo manual.
72	Difusores de bulbo de ambiente cerrados.
74	Difusores de bulbo falso suelo cerrados.
14	Difusores abiertos.
2	Indicadores óptico-acústicos de extinción disparada.
11	Extintores manuales CO_2 34B.
14	Extintores manuales Polvo 21A.
5	Bocas de Incendio Equipadas (BIE).

En el almacén existe una instalación realizada con varios splitter en el techo que pueden descargar agua, cuya puesta en marcha es manual.

Para todos los componentes existen los correspondientes contratos de mantenimiento con empresas externas que se revisan anualmente.

Para su manejo iremos a la Guía de Sistemas de Extinción

4.4. Alarmas de control de acceso y vídeo vigilancia

La alarma de control de acceso y vídeo vigilancia del Centro Informático está compuesta por:

- *Control de Acceso*

1 Software de Control de Acceso (Visor).
8 Lectores de tarjeta de proximidad.
5 Cerraduras eléctricas a emisión corriente, para puertas cortafuegos.
1 Lector de códigos de tarjetas.

- Video Vigilancia

1 Software de Video Vigilancia (Visor)
6 Conjunto de cámara fijas
3 Conjuntos de cámara DOMO

Para su manejo iremos a la Guía usuario control acceso.

4.5. Control de la puesta en marcha del Grupo Electrógeno (cortes de luz)

Se deberá ***anotar los siguientes datos en el Parte de Servicio.***

- Cuántos cortes de luz se producen.
- Hora de cada corte de luz en formato HH:MM y su duración.
- Cuántas veces entra en funcionamiento el Grupo Electrógeno y durante cuanto tiempo.

En caso de que haya un corte en el suministro de la corriente eléctrica y no funcione correctamente el sistema automático: Seguir la Guía de arranque y conmutación manual del grupo electrógeno.

4.6. Aire Acondicionado

La forma de actuar ante una incidencia será:

- Cuando se perciba algo extraño “se llamará al técnico de la empresa externa encargada del mantenimiento del Aire Acondicionado” facilitándole todos los datos de la incidencia y respondiéndole a las preguntas que haga.
- Los técnicos de la empresa externa encargada del mantenimiento del Aire Acondicionado son los responsables del A/A ***siendo ellos los que tienen que valorar si han de venir o no al centro.***

  El personal de seguridad tiene la responsabilidad de llamar y no desentenderse del problema. Es decir, que si por ejemplo el técnico le dijera al vigilante que vuelva a llamar más tarde, lo haga. O por ejemplo, si el técnico tiene que volver a llamar y no lo hace, sea el vigilante el que insista.

- Cuando finalice su estancia en el centro “deberá informar al vigilante del estado en que se queda el A/A (si el trabajo está terminado, si tiene que traer alguna pieza y mientras tanto se debe controlar la máquina, etc.…).

  El servicio de seguridad informará al encargado de mantenimiento o en su defecto a la dirección del centro dejando constancia en el Parte de Servicio.

  Los albaranes se entregarán a la persona encargada de mantenimiento.

- **Es conveniente asegurarse, tras la estancia de trabajadores de otros gremios en la UPS, de que el A/A están funcionando convenientemente.** Pudiera ser que se hubiese apagado el aire para realizar ciertos trabajos y olviden conectarlos de nuevo.

Para su manejo iremos a los Manuales de las máquinas de Aire Acondicionados.

4.6.1 Temperatura Sala CPD (máxima 27º)

Si se detectara 27º o más en cualquiera de los 3 termómetros avisar al responsable de mantenimiento y, si el pasillo circundante está más fresco que la sala, abrir las puertas de la sala para regular la temperatura.

Para controlar las temperaturas, efectuaremos una foto de los termómetros con la cámara asignada al servicio de vigilancia, con la siguiente frecuencia:

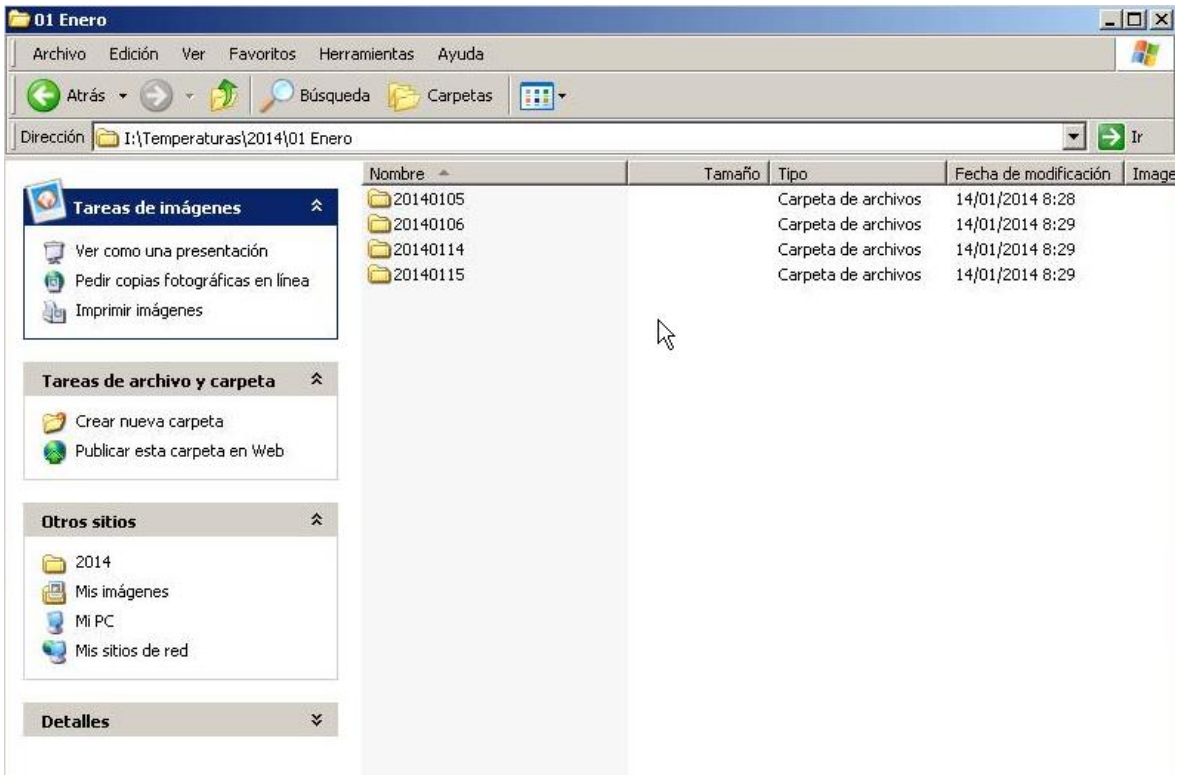
En días laborables:

- En el turno de tarde de 15:00 a 23:00, realizaremos dos capturas.
- En el turno de noche de 23:00 a 7:00, realizaremos dos capturas.

En días festivos y fines de semana:

- En el turno de día de 7:00 a 19:00, realizaremos tres capturas.
- En el turno de noche de 19:00 a 7:00, realizaremos tres capturas.

Será de obligado cumplimiento que, tras la toma de la foto y mediante el cable de datos, realicemos la transferencia de la imagen a la carpeta creada al efecto y denominada ***TEMPERATURAS***. Se asignará en el año, mes y día correspondiente. Además, se adjuntará la imagen al parte diario de incidencias, previa anotación de la temperatura en el mismo.



NOTA: Antes de usar la cámara de fotos deberemos comprobar que esta correcta la fecha de la cámara

4.7. Agua Nebulizada

Se comprobará que los manómetros del agua nebulizada estén uno de ellos en la zona verde y los dos restantes sobre los 180 bar (si está por encima de los 200 no pasa nada, tiene mayor capacidad. Lo normal es que esté entre los 190 y 200 bar (son más fiables estos dos manómetros últimos que el del color verde). Se informará a la persona encargada del mantenimiento del centro ante cualquier incidencia que se registre al respecto.

Para su manejo iremos a las Guías de Extinción.

4.8. Compuertas Cortafuegos (armario frente a C. Transf.)

Hay instalados unos pilotos que están en verde si las compuertas están abiertas y en rojo si han saltado. Que estén en verde es lo habitual.

5. ANEXO

5.1. 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 (RGPD):

No tirar ningún papel con información/datos a la papelera, reservarlos en la zona habilitada para ello en búnker de vigilantes para cuando sea oportuno subirlos a impresoras para su destrucción.

5.2. Aviso de confidencialidad “DATOS PERSONALES”

La utilización, divulgación y/o copia sin autorización está prohibida en virtud de la legislación vigente (RGPD y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales). No puede proceder a su tratamiento o comunicación a terceros sin el previo consentimiento del interesado.



5.3. Ley Foral 6/2003, de 14 de Febrero, de prevención del consumo de tabaco, de protección del aire respirable y de la promoción de la salud en relación al tabaco.

La presente Ley Foral tiene por objeto la adopción de medidas reguladoras de actuaciones dirigidas a establecer un adecuado nivel de protección de la salud frente a los riesgos derivados del consumo de tabaco, a la prevención del inicio de su consumo y a la promoción de hábitos saludables para la mejora de la calidad de vida de la ciudadanía.

5.4. Avisos a los cuerpos de Seguridad del Estado

ANTES DE LLAMAR DEBE RELLENARSE ESTE FORMULARIO Y SEGUIRLO PARA UN INFORME COMPLETO A LA POLICÍA

LE LLAMA EL SERVICIO DE SEGURIDAD PRIVADA DE

Centro Informático del Gobierno de Navarra

PRESTADO POR
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

SOY EL VIGILANTE DE SEGURIDAD	PRIMER APELLIDO	
	SEGUNDO APELLIDO	
	NOMBRE	
	NUMERO DE LA TARJETA DE IDENTIDAD PROFESIONAL	

LES INFORMO QUE HA SUCEDIDO LO SIGUIENTE

¿QUÉ HA SUCEDIDO?							
ROBO		A PERSONA		DE BIENES		DE VEHÍCULO	
SOSPECHOSO		SECUESTRO		DERRUMBE		AMENAZA DE BOMBA	
INTRUSIÓN		ATENTADO		INCENDIO		POSIBLE BOMBA	
		TIROTEO				EXPLOSIÓN	

¿CUÁNDO HA SUCEDIDO?							
DÍA		HORA		SE IGNORA			

¿DÓNDE HA SUCEDIDO?

¿QUIÉN ESTÁ RELACIONADO?						
VÍCTIMAS	NUMERO		CON DAÑOS		SIN DAÑOS	
PRESUNTOS AUTORES	NUMERO		DETENIDOS		SOSPECHOSOS	
TESTIGO	NÚMERO		LOCALIZADO			

¿POR QUÉ SE HA CONOCIDO LO QUE HA SUCEDIDO?			
INTERVENCIÓN DE LOS VIGILANTES		DENUNCIA DE PERSONAL RESIDENTE	
CENTRAL RECEPTORA DE ALARMAS			

¿QUÉ MEDIDAS SE HAN ADOPTADO?			
DETENCIÓN DEL (O LOS) PRESUNTOS RESPONSABLES		DESCRIPCIÓN DEL (Ó LOS) PRESUNTOS RESPONSABLES	
AISLAMIENTO DE LA ZONA		RECUPERACIÓN DE EFECTOS	
LLAMADA A LOS BOMBEROS		LLAMADA A UNA AMBULANCIA	
CUIDADOS A LOS HERIDOS			

SE DISPONE DE **DESCRIPCIONES DE PRESUNTOS AUTORES, Ó PERSONAS Y VEHÍCULOS SOSPECHOSOS**, ESCRIBA SUS CARACTERÍSTICAS EN LA PARTE DE ATRÁS DE ESTA HOJA Y COMUNÍQUELO TAMBIÉN A LA POLICÍA

DESCRIPCIONES DE PRESUNTOS AUTORES Ó SOSPECHOSOS					
	1	**2**	**3**	**4**	**5**

DESCRIPCIONES DE PRESUNTOS AUTORES Ó SOSPECHOSOS						
ESTATURA						
COMPLEXIÓN						
FACCIONES						
TIPO DE ROPA						
COLOR DE LA ROPA	SUPERIOR					
	PANTALÓN					
CUBRECABEZAS						
GAFAS						
CALZADO						
OBJETOS						
OTROS DETALLES						

EXPLICACIONES

ESTATURA: ALTO, MEDIANO, BAJO. (PRECISAR MÁS SÍ SE PUEDE)
COMPLEXIÓN: FUERTE, DELGADO, GRUESO
FACCIONES: EUROPEAS, AMERICANAS, NORTEAFRICANAS, CENTROAFRICANAS, ETC.
TIPO DE ROPA: DEPORTIVA, MONO, TRAJE, ETC.
COLOR DE ROPA: LA PRENDA SUPERIOR, EL PANTALÓN, ETC.
CUBRECABEZAS: PASAMONTAÑAS, GORRA DE VISERA, BOINA, SU COLOR
GAFAS: DE SOL, NORMALES, FINAS, GRUESAS, ETC.
CALZADO: DEPORTIVO, DE MONTAÑA, SU COLOR
OBJETOS: BOLSAS, PAQUETES, MAZAS CIZALLAS, ARMAS, ETC.
OTROS DETALLES: AÑADIR TODO LO QUE COMPLETE LA IDENTIFICACIÓN, COMO TATUAJES, PENDIENTES, PIERCING, LUNARES, ETC.

DESCRIPCIÓN DE VEHÍCULOS SOSPECHOSOS					
	1	**2**	**3**	**4**	**5**
MATRÍCULA					
COLOR					
MARCA					

MODELO					
ESTADO					
OTROS DETALLES					

EXPLICACIONES:

MATRÍCULA: TENER EN CUENTA LOS POSIBLES TIPOS ESPAÑOLES (ZZ 1234 AA, 3456 AAA) Y LOS TIPOS EXTRANJEROS

ESTADO: NUEVO, MEDIANO USO, VIEJO

OTROS DETALLES: GOLPES, ARAÑAZOS, PEGATINAS Y SU UBICACIÓN

EL VIGILANTE DE SEGURIDAD		
PRIMER APELLIDO		**FIRMA**
SEGUNDO APELLIDO		
NOMBRE		
FECHA		

OFREZCA ESTE FORMULARIO A LA POLICÍA

5.5. Comunicaciones

5.5.1 Generalidades

Las comunicaciones sólo se utilizarán para tramitar los asuntos relativos al funcionamiento del Servicio de Seguridad.

Las comunicaciones por radio serán efectuadas teniendo presente la posibilidad de que otros receptores ajenos al Servicio de Seguridad puedan captar los mensajes. Por lo tanto, no se dará ninguna referencia explícita al estado de la seguridad, personal, ubicación de los vigilantes, dirección, propósito, etc.

Para identificar a las personas se utilizará la denominación abreviada de sus cargos, de sus Departamentos o referencias anónimas a las personas.

Solo cuando se pueda inducir al error o a la confusión se personalizará la referencia verbal y siempre con carácter excepcional.

Es preciso tener en cuenta que las conversaciones del Servicio de Seguridad deben realizarse siempre con normalidad y utilizando expresiones que (aunque se refieran a situaciones de alarma o emergencia) no provoquen dudas o nerviosismo en las personas situadas alrededor. Por ello, se establece, ***en el punto 5.5.4,*** un lenguaje convenido que podrá incrementarse según convenga.

En cualquier conversación, y especialmente en las emergencias, es muy importante que, a fin de que el interlocutor (cuerpos de seguridad del Estado, bomberos, etc.,), comprenda lo que se le está comunicando, y se transmita la comunicación con:

- ***CLARIDAD DE CONCEPTOS.***
- ***CALMA, EXACTITUD Y BREVEDAD.***
- ***SONORIDAD Y VELOCIDAD ADECUADAS***.

Antes de transmitir la información, deben averiguarse los mayores detalles:

- ***¿QUE HA PASADO?***
- ***¿CUANDO HA PASADO?***
- ***¿DÓNDE HA PASADO?***
- ***¿QUIEN ESTA RELACIONADO CON LA EMERGENCIA?***
- ***¿POR QUÉ HA SUCEDIDO?***
- ***¿QUÉ MEDIDAS HAN SIDO YA ADOPTADAS?***

5.5.2 Por radio

En este servicio no se utiliza una red radio para sus comunicaciones internas.

5.5.3 Por teléfono

En este servicio no se utiliza la red telefónica particular para sus comunicaciones internas.

5.5.4 Lenguaje convenido

SITUACION	**CODIGO**
NORMAL	BRAVO VERDE

ALERTA	BRAVO AMARILLO
EMERGENCIA, PELIGRO	BRAVO ROJO
EMERGENCIA CON VICTIMAS	BRAVO ORO

5.5.5 Hechos Ocurridos

HECHOS OCURRIDOS	**CODIGO**
ALBOROTO	RUIDO
PERSONA SOSPECHOSA	CARA
PAQUETE SOSPECHOSO	BULTO
VEHICULO SOSPECHOSO	CARRO
INTRUSION	BAILE
CAIDA	GOLPE
PERCANCE EN INSTALACIONES	ROTO
ATROPELLO	ROTURA
HURTO , ROBO	NOCHE
OBJETO PELIGROSO	CORTANTE
INCENDIO	ROJO