Aprobado en Consejo de Administración el día 27 de octubre de 2023

PROTOCOLO DE SEGURIDAD INFORMÁTICA EN GORONA DEL VIENTO EL HIERRO, S.A.

Revisión: 01

INDICE

1 INTRODUCCIÓN

El presente Protocolo tiene como objetivo mejorar el uso de los sistemas informáticos por todos sus usuarios en GORONA, haciendo especial hincapié en la seguridad, en la ética del uso de los ordenadores en el trabajo, en la prevención de delitos informáticos y en la prevención de riesgos.

Este Protocolo debe ser de lectura **obligada** por parte de cualquier miembro o colaborador de GORONA, con el fin de prevenir de los peligros más habituales a los que están expuestos hoy en día y establecer unas pautas de control dentro de la Empresa y que sus usuarios sean conscientes de lo que deben hacer (y no deben hacer) para el correcto funcionamiento de su sistema informático, tanto a nivel de seguridad, como a nivel de uso de la información, como a nivel de cumplimiento y ética profesional en sus horas de trabajo.

2 OBJETIVOS

Las directrices y principios que se contienen en el presente Protocolo, tienen como objetivo conseguir que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso para asegurar su correcta funcionalidad, brindando un nivel de seguridad optimo y que permitan:

- Disminuir las amenazas a la seguridad de la información y los datos.
- Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.
- Cuidar y proteger los recursos tecnológicos de GORONA.
- Concientizar a sus usuarios sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.

3 ALCANCE

Las disposiciones y principios del presente documento, aplica a sus empleados, directivos, contratistas, asesores, personal de apoyo y terceros no vinculados directamente a GORONA, pero que presten su servicio y utilicen tecnología de información, equipos propios GORONA o arrendados y a los equipos de personas externas que sean conectados a la red de GORONA.

La revisión de este Protocolo, debe realizarse con una periodicidad mínima de una vez al año o cuando se originen cambios en la entidad que puedan afectar la operación de los servicios, o durante las revisiones periódicas que se ejecuten para asegurar la continuidad del sistema.

4 RESPONSABILIDADES

4.1 En general:

Todos los empleados, directivos y colaboradores de GORONA tienen la responsabilidad de proteger la seguridad de los activos y de los recursos bajo su control, de acuerdo con las instrucciones y la capacitación recibidas.

Deben definirse responsabilidades expresas para la implementación, operación y administración de los controles de seguridad informática y discriminarse dichas responsabilidades de aquellas que sean incompatibles, cuando esto pudiera debilitar el nivel del control interno en forma inaceptable.

4.2 La Secretaría General Técnica:

La Secretaría General Técnica (SGT) será la responsable de tecnología y sistemas de la información, la cual se encargará de:

- Desarrollar, revisar y actualizar las políticas de seguridad informática.
- Acordar las prioridades de seguridad informática.
- Coordinar la implementación de dichas políticas.
- Monitorear e informar sobre el trabajo de seguridad informática a los órganos de administración de GORONA;
- Dar asesoramiento sobre la seguridad física de todas las instalaciones.
- Garantizar que la seguridad de todos los activos esté debidamente protegida.
- Definir los principios de gestión de acceso que permitirá únicamente el ingreso a los usuarios autorizados por la dependencia correspondiente, y en el nivel asignado, sobre los datos, la red y sistemas de información necesarios para desempeñar sus tareas habituales.
- Definir las directrices de contraseñas robustas para los usuarios de las Bases de Datos, Red y Sistemas de Información.

- Definir las herramientas, procedimientos, formatos entre otros, para la implementación de un sistema de autenticación de acceso a los usuarios internos y externos en las diferentes plataformas tecnológicas.
- Definir las herramientas, procedimientos de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.
- Garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de GORONA por medio de los terceros autorizados.
- Proveer las herramientas tales como antivirus, antimalware, anti spam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica GORONA y los servicios que se ejecutan en la misma.
- Establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente.
- Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- Validar los riesgos que genera la migración hacia nuevas versiones del software operativo.
- Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos.
- Realizar el borrado seguro del contenido de medios reutilizables que contengan información reservada de GORONA que se van a retirar de las instalaciones.
- Realizar respaldo a través del proceso de gestión de copias de respaldo de la información reservada, cuya duración es mayor al tiempo de vida del medio en donde se encuentra almacenada.
- Realizar pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, a través de un tercero, que cumplan con estándares internacionales.
- Generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
- Proponer políticas y especificaciones técnicas de bienes y servicios, procedimientos, acciones y medidas específicas en materia de Seguridad Informática.

- Coordinar la administración del sistema de autentificación de usuarios que permite el acceso a los recursos, servicios informáticos y comunicaciones de GORONA.
- Proponer medidas específicas en materia de Seguridad Informática que deberán atender los usuarios de los bienes, de los recursos y servicios informáticos y de la información electrónica.
- Mantener actualizado el inventario de Activos Informáticos relacionados con la Plataforma de Seguridad Informática de GORONA, como complemento del inventario de activos de Información e infraestructura con que esta cuenta.
- Realizar revisiones selectivas a los controles de los activos informáticos para asegurar que se mantenga sobre ellos la aplicación de las recomendaciones y directrices en materia de Seguridad Informática;
- Revocar las contraseñas, cuando las claves estén comprometidas o cuando un usuario que haga uso de ellas se desvincule de la entidad;
- Recuperar las contraseñas perdidas o alteradas como parte de la administración para su continuidad;
- Coordinar, administrar y registrar todos los nombres de equipos y dominios que son accesibles a la red de GORONA;
- Controlar y registrar todos los certificados de seguridad de los sitios de la entidad.

4.3 El personal de GORONA y los Colaboradores

Todo el personal y los colaboradores externos de GORONA son responsables de:

- Cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad específicas documentadas en los objetivos personales y la descripción de tareas;
- Mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados;
- Proteger la seguridad de los equipos informáticos, así como de la información bajo su control directo;
- Informar a la SGT de cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de esta, incluyendo sospechas de divulgación de contraseñas;
- Acatar con las directrices establecidas dentro de este documento.

5 DIRECTRICES

5.1 En general

a. Las presentes directrices se dictan con el objeto gestionar adecuadamente la tecnología y los sistemas informáticos de GORONA.
b. Toda movilización del activo informático dentro o fuera de las instalaciones de GORONA, es responsabilidad del personal asignado a este.
c. Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa a un activo informativo, deberá ser notificado de inmediato a la SGT, la que informara de las acciones a tomar.
d. Solo el personal designado por la SGT está autorizado a realizar reparaciones, cambios o desarme de los activos informáticos de GORONA.
e. La SGT realizara periódicamente actualizaciones a los sistemas operativos, parches de seguridad, antivirus y de las aplicaciones instaladas en los PCs de escritorio y portátiles del personal de GORONA, quienes deben garantizar el reinicio de estos para su ejecución.
f. Todos los activos tecnológicos propiedad de GORONA deberán estar incluidos dentro del dominio www.goronadelviento.es y aplicar las políticas de seguridad definidas por la SGT tales como p.e.: un fondo de pantalla definido, acceso al activo tecnológico de acuerdo con su perfil, bloqueo a las propiedades del sistema operativos, entro otros.
g. Todo activo tecnológico que no se encuentre dentro del dominio o no cuente con las políticas de seguridad definidas por la SGT, será solicitado al personal de GORONA. De negarse a entregar el activo tecnológico se informará a la SGT para que tome las acciones pertinentes.
h. El personal de GORONA con activos tecnológicos no debe cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la SGT y únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

5.2 Internet:

La SGT provee el servicio de internet al personal de GORONA para desarrollar exclusivamente las funciones asignadas a su cargo, debiendo utilizarse de forma austera y eficiente.

Será de aplicación al personal de GORONA y sus colaboradores externos, las directrices siguientes:

a. Abstenerse de publicar Información relevante a GORONA independiente de su formato (Word, Excel, Power Point, PDF, avi, mp3, mp4 o cualquier otro formato actual o futuro) o su nivel de clasificación de confidencialidad en sitios de internet no licenciados por GORONA en los denominados discos, nubes, carpetas virtuales o cualquier sistema de publicación de documentos actual o futura dentro o fuera de la entidad.
b. Inhibirse de utilizar aplicaciones que permitan evadir los controles implementados por GORONA.
c. El acceso a páginas Web con contenido inapropiado se encuentra restringido. Sin embargo y si por la naturaleza del cargo se requiere el acceso a páginas de acceso contralado, se debe solicitar a la SGT su acceso adjuntando la aprobación y justificación por parte del jefe inmediato.
d. Abstenerse de descargar imágenes, sonidos, música y videos, a su vez descargar archivos o instalar programas de sitios web desconocidos o gratuitos.
e. La SGT se reserva el derecho de bloquear sitios que se detecten como peligrosos (con contenidos no autorizados) para la seguridad de los activos informáticos.
f. Cada persona es responsable del adecuado manejo de los usuarios de autenticación y contraseña a la hora de ingresar a los diferentes sistemas de información que consulte en internet.
g. El correo electrónico institucional es para uso exclusivo del personal de GORONA, por lo cual deberá ser utilizado solo para realizar actividades relacionadas con sus funciones.
h. La SGT garantizara mediante políticas en los activos informáticos el apagado de estos en el horario establecido por GORONA.
i. Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor y tal efecto todos los colaboradores se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor y que no se encuentren licenciados por parte de GORONA.
j. Para asegurarse de no violar los derechos de autor, no está permitido a los colaboradores copiar ningún programa instalado en los activos informáticos de la entidad en ninguna circunstancia sin la autorización escrita de la SGT.
k. No está permitido instalar ningún programa en el activo informático sin dicha autorización o la clara verificación de que GORONA posee una licencia que cubre dicha instalación.
l. No está autorizada la descarga de Internet de programas informáticos no autorizados por SGT. De ser necesario por cualquier área de GORONA, se debe solicitar por medio de la SGT.

m. No está permitido que se realicen copias no autorizadas de programas informáticos, cualquier tipo de información, sistemas de información, base de datos, etc.
n. No está permitido que se carguen o descarguen programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos para utilizar sistemas de peer-to-peer (P2P – Ej. Kazaa) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.
o. No está permitido que los colaboradores realicen intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor.
p. Si se evidencia que alguna persona ha realizado copia de programas informáticos o música en forma ilegal, la SGT comunicara al jefe inmediato para que este tome las medidas necesarias.
q. GORONA provee a su personal licencia de Office 365 para su uso laboral, asociada a la cuenta de correo de GORONA. El uso de esta licencia en dispositivos personales como portátiles o teléfonos estará supeditada a la autorización expresa de GORONA. Esta licencia no puede ser cedida, vendida o alquilada.
r. Si un usuario desea utilizar programas informáticos autorizados por GORONA en su hogar, debe consultar y obtener autorización de la SGT.
s. El personal de la SGT revisará los activos informáticos constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si los colaboradores poseen licencias para cada una de las copias de los programas informáticos instalados.
t. Si se encuentran programas informáticos sin licencias, licencias free, licencias no corporativas, etc., estas serán eliminadas y, de ser necesario, reemplazadas por programas informáticos con licencia con que cuente GORONA.
u. Los que se enteren de cualquier uso inadecuado que se haga en GORONA con los programas informáticos o la documentación vinculada a estos, deberán notificarlo a la SGT.

5.3 Correo electrónico, bases de datos y contraseñas

a. La creación de usuarios de correos, bases de datos y sistemas de Información se debe realizar a través de una solicitud a la SGT, según el modelo del Anexo II de este documento.

b. El sistema de administración de contraseñas para usuarios de correo, bases de datos, sistemas de información y redes de GORONA se atendrá a lo indicado en la Política de Gestión de Contraseñas (ver Anexo V), y será obligatorio el uso de usuarios y contraseñas individuales para determinar responsabilidades.

c. La administración y buen uso de contraseñas es responsabilidad de cada usuario de correo, Bases de Datos, Sistemas de Información, redes y deben estar alineadas con la política de uso y creación de contraseñas seguras.

d. Las contraseñas deben estar almacenadas en un sistema informático protegido mediante tecnologías diferentes a las utilizadas para la identificación y autenticación de usuarios.

e. El personal de GORONA y los colaboradores deben proteger sus contraseñas conforme con las recomendaciones contenidas en la Política de Gestión de Contraseñas (ver Anexo V).

f. Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

g. Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

h. Si los sistemas de información detectan inactividad por un periodo igual o superior a cinco (5) minutos, deben automáticamente finalizar la sesión de usuario.

i. Los colaboradores usuarios de correo, bases de datos, sistemas de información y redes se encuentran afectados por las directrices siguientes:

- Asumir la responsabilidad de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

- No compartir sus cuentas de usuario y contraseñas con otros colaboradores o con personal provisto por terceras partes.
- A los que les fuese asignada una cuenta y contraseña de otras entidades deberán cumplir con las políticas de GORONA, así como las políticas de seguridad de la entidad que asigna dicha cuenta.
- Los que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de GORONA deben acogerse a directrices y políticas para la configuración de cuentas de usuario y contraseñas implantados por GORONA.

a. Las cuentas creadas en los dominios de GORONA, se ajustarán a las directrices siguientes:
   - Serán bloqueadas automáticamente después de estar inactiva en un tiempo de sesenta (60) días.
   - Serán eliminadas automáticamente después de estar inactivas en un tiempo de noventa (90) días.
   - Serán administradas por la SGT.

b. Toda la información de GORONA deberá únicamente ser operada a través de las bases de datos y sistemas de información implantados por GORONA, para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse algún fallo.

c. El acceso a los sistemas de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de GORONA. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

d. Se deben delimitar las responsabilidades en cuanto a quien está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.

e. Los datos de los sistemas de información deben ser respaldados de acuerdo con la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados.

f. En cuanto a la información de los equipos de cómputo suministrados a los colaboradores, se recomienda a los usuarios que realicen sus propios respaldos en una aplicación de respaldo.

g. Los sistemas de información deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó.

h. Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

5.4 La red

a. El acceso de los colaboradores a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:
   - Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.
   - Se exige control de acceso de los usuarios a los servicios de información.
   - Mantener instalados y habilitados solo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad.
   - Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad.
   - El acceso de las redes de GORONA es de uso exclusivo y único para la infraestructura provista.

b. Debe presidir el control de acceso de los usuarios a las redes las directrices siguientes:
   - El personal de GORONA únicamente deben tener permiso de acceso directo a las aplicaciones y bases de datos, para cuyo uso están específicamente autorizados.
   - Todos los accesos de los usuarios remotos a sistemas y aplicaciones de información deben estar controlados por medio de autenticación.
   - Todas las conexiones remotas que se realicen a sistemas de información deben ser autenticadas.
   - Los puertos empleados para diagnóstico remoto y configuración deben estar controlados de forma segura, deben estar protegidos a través de un mecanismo de seguridad adecuado y un procedimiento para asegurar que los accesos lógicos y físicos a estos son autorizados.

- La autenticación de usuarios remotos deberá ser aprobada por el jefe inmediato del colaborador y bajo una solicitud con su respectivo formato.

c. Los medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos deberán contener, como mínimo, las características siguientes:
   - Autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;
   - Registrar intentos exitosos y fallidos de autenticación del sistema;
   - Emitir alarmas cuando se violan las políticas de seguridad del sistema;
   - Suministrar medios adecuados para la autenticación cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

d. Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de GORONA entre los Colaboradores, departamentos, oficinas y hacia afuera a través de conexiones con otras redes u otras entidades y a tal efecto, se estable que:
   - La SGT no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el personal o Colaborador que los genere o solicite.
   - Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
   - No se permite el uso de los servicios de la red cuando no cumplan con las labores propias dentro de GORONA.
   - Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de GORONA y se usarán exclusivamente para actividades relacionadas con la labor asignada.
   - Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
   - La SGT es el único que cuenta con permisos para el uso de analizadores de red los cuales son usados para monitorear la funcionalidad de las redes.
   - No se permitirá el uso de analizadores para monitorear o censar redes ajenas a GORONA y no se deberán realizar análisis de la Red desde equipos externos a la entidad.
   - Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al personal, Colaborador o

red involucrada. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.
- Los servicios hacia Internet solo podrán proveerse a través de los servidores autorizados por la SGT.

5.5 Trabajo Remoto

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones de GORONA.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles está restringido únicamente a los provistos por la institución, atendiendo al Protocolo para el teletrabajo en Gorona del Viento El Hierro, S.A., y contemplan las siguientes directrices:

- El trabajo remoto solo es autorizado por el responsable de la unidad organizativa de la cual dependa el colaborador que solicite el permiso.
- Dicha autorización solo se otorgará por la SGT, una vez se verifique las condiciones de seguridad del ambiente de trabajo.
- Se utilizará la conexión de acceso remoto solo para acceder a servicios (File server, diferentes aplicativos, infraestructura entre otros) exclusivos de GORONA, los cuales sean inalcanzables desde redes externas.
- Solo se permitirá las conexiones remotas a los recursos de la plataforma tecnológica a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- La SGT suministrará las herramientas y controles necesarios para realizar conexiones de manera segura.
- La SGT monitoreará las conexiones remotas a los recursos de la plataforma tecnológica de GORONA de manera permanente.
- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de GORONA y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Los usuarios únicamente deben establecer conexiones remotas a través de las VPN seguras y utilizar computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

5.6 Medios Removibles

Un adecuado uso de los medios removibles recomienda tener en cuenta las directrices siguientes:

- El contenido de medios reutilizables que contengan información crítica o sensible que se van a retirar de las instalaciones, se les deberá realizar un borrado seguro. Para el retiro de dichos medios se debe contar con la autorización de la SGT.
- La información crítica o sensible cuya duración es mayor al tiempo de vida del medio en donde se encuentra almacenada, deberá respaldarse a través del proceso de gestión de copias de respaldo para evitar la pérdida de información.
- El colaborador debe asegurar el resguardo de la información contenida en el medio removible que le fue asignado.
- El colaborador debe dar buen uso a los medios removibles asignados, informando en forma oportuna cualquier deterioro.
- Se debe de garantizar la integridad y disponibilidad de la información almacenada en medios removibles, cambiando de contenedor cuando culmine el tiempo de vida.
- Es de exclusiva responsabilidad de cada persona tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles. Evitando accesos no autorizados, daños, pérdida de información o extravío del medio.
- En caso de ocurrir perdida, modificación o daño de la información o del medio, se debe informar al Oficial de seguridad o quien haga sus veces.

5.7 Redes Privadas Virtuales (VPN)

Los usuarios móviles y remotos de GORONA podrán tener acceso a la red interna privada cuando se encuentren fuera de esta con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por la SGT.

La SGT será la encargada de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

La persona de GORONA o el colaborador que solicite una VPN es responsable del acceso remoto y del uso de este.

Para que un colaborador o proveedor de GORONA pueda acceder a los equipos, ya sean servidores u otros equipos de la red interna de GORONA desde una conexión externa con la tecnología VPN, cumplirá con el siguiente procedimiento:

- El Colaborador o proveedor solicitará el acceso remoto mediante al servicio.
- La solicitud deberá incluir el formato con la justificación para la solicitud de este acceso e indicará el tiempo requerido para el mismo, la información completa de la conexión y la información del aprobador de la solicitud. Esto aplica a todos los colaboradores y proveedores que tiene que realizar tareas fuera de horas laborables o en instalaciones que necesiten este tipo de acceso, participar en proyectos que requieran apoyo remoto, o alguna otra circunstancia especial que así lo amerite.
- La SGT evaluará la solicitud; si aprueba la misma, se procederá a otorgar los permisos y acceso a la VPN. De no aprobar la misma, se devuelve al colaborador o proveedor solicitante con las razones de la decisión.
- Una vez procesado el permiso, se notifica al Colaborador o proveedor y se le dan las instrucciones para conectarse vía VPN. Si es necesario, personal técnico asistirá al usuario en el proceso de configurar el VPN.

5.8 Red Inalámbrica (WIFI)

La red inalámbrica es un servicio que permite conectarse a la red de la entidad e Internet sin la necesidad de algún tipo de cableado. La red inalámbrica le permitirá utilizar sus servicios en las zonas de cobertura de esta, donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.

Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, IPod, celulares, etc.) con capacidad de conexión Wireless.

La SGT es la encargada de la administración, habilitación y/o bajas de usuarios en la red inalámbrica dentro de GORONA

La red inalámbrica de invitados es un servicio que permite conectarse única y exclusivamente a personal externo (clientes, proveedores, visitantes) a internet sin la necesidad de algún tipo de cableado.

Los usuarios invitados no tendrán acceso a la red de GORONA ni a ningún recurso de uso privado de la entidad.

6 SEGURIDAD

6.1 En general

El personal de GORONA y los Colaboradores deben cumplir con los principios de seguridad siguientes:

- Ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Deben garantizar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los que sospechen o detecten alguna infección por software malicioso deben notificar a la SGT para que tome las medidas de control correspondientes.
- Deben realizar copias de la información reservada de GORONA, mediante el uso de los puertos de los computadores, a cualquier dispositivo de almacenamiento externo (CD's, DVD's, discos duros externos, memorias USB, etc.).
- Generar contraseñas robustas para las Bases de Datos, Red y Sistemas de Información.
- Utilizar las herramientas, procedimientos, formatos entre otros, para la implementación de un sistema de autenticación de acceso a los usuarios internos y externos en las diferentes plataformas tecnológicas.
- Velar porque el personal provisto por terceras partes tenga acceso únicamente a la información necesaria para el desarrollo de sus labores y garantizará que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.
- Utilizar las herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de GORONA y los servicios que se ejecutan en la misma.

- Permitir las actualizaciones de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de GORONA.
- Solicitar borrado seguro del contenido de medios reutilizables que contengan información reservada de GORONA que se van a retirar de las instalaciones.
- Realizar copias periódicas de la información correspondiente a sus funciones dentro de GORONA.
- Comunicar cualquier caso de vulnerabilidad dentro de los sistemas de información de GORONA.

6.2 Seguridad Perimetral

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

GORONA implementará soluciones lógicas y físicas que garanticen la protección de la información de GORONA de posibles ataques internos o externos, rechazando conexiones a servicios comprometidos, permitiendo solo ciertos tipos de tráfico (p. ej. correo electrónico, http, https), proporcionando un único punto de interconexión con el exterior y redirigiendo el tráfico entrante a los dispositivos de seguridad con que cuenta GORONA. Asimismo, deberá ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet, auditar el tráfico entre el exterior y el interior y ocultar información de nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

6.3 Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

6.4 Seguridad física y ambiental en instalaciones

Las instalaciones con fines específicos que alberguen equipos de procesamiento, almacenamiento, conectividad, seguridad críticos requieren una mayor protección que la proporcionada a las instalaciones comunes. El acceso a los centros de cómputo y centros de cableado es restringido.

Solo el personal autorizado por el operador de servicios cuenta con el acceso a los gabinetes (racks) donde se encuentre alojada infraestructura de procesamiento, almacenamiento, networking y seguridad. Si alguna área requiere el acceso a estos gabinetes (rack) se debe solicitar de la SGT.

No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la entidad, a menos que esté autorizado.

7 RIESGOS INFORMÁTICOS

A la vista del análisis realizado por una consultaría externa, estos son los principales problemas de seguridad informática de GORONA:

- Acceso al contenido de cuentas de correo empresariales por parte de hackers informáticos o suplantación de identidad sobre todo en el procedo de pagos/cobros de facturas.
- Encriptación de documentos por virus informático.
- Pérdida de datos de GORONA por errores propios o por usuarios malintencionados.
- Acceso a datos confidenciales de personas no autorizadas.
- Extracción de información confidencial o estratégica por parte de espías informáticos.
- Acceso a cuentas e informaciones personales.
- Compras y estafas en páginas web fraudulentas.
- Engaños informáticos a través del correo.
- Engaños informáticos a través de una página web.
- Descarga de virus y archivos dañinos en páginas web.

7.1 Suplantación de identidad.

Un problema habitual hoy en día es la suplantación de identidad en el ámbito de Internet, que es básicamente hacerse pasar por otra persona. Este delito es muy frecuente y esta principalmente asociado a cuentas de correo electrónico empresariales y tiene como único objetivo conseguir dinero de forma ilícita.

Dentro de las suplantaciones de identidad destacamos la práctica "Man in the middle" que se produce de forma constante y puede ocasionar una pérdida importante de dinero. Todo se inicia cuando abrimos un correo electrónico que contiene un virus que no afecta al funcionamiento del equipo, pero es capaz de descifrar la contraseña del correo. Una vez la clave del correo está al alcance del hacker, se queda a la escucha y monitoriza el correo del usuario a la espera de un posible negocio. Cuando ve una oportunidad de negocio, por ejemplo, el pago de una factura es cuando actúa. El hacker se mete de lleno en la conversación y se hace pasar por la empresa que emite la factura, indicando que ha habido un cambio en el número de cuenta y que el ingreso del importe lo deben realizar a una cuenta concreta (la del propio hacker). El usuario que recibe esta petición la atiende normalmente y realiza el ingreso del importe en una cuenta que no es la correcta. A partir de ahí, empiezan disputas entre los dos usuarios por ver quien tiene la responsabilidad, pero el mal ya está hecho, porque suelen ser cuentas extranjeras que cuando se reclama el dinero ya no están operativas en muchos casos. Este sistema que parece a priori poco peligroso, debido al gran volumen de facturación y al ajetreo del día a día, se ha podido comprobar que es muy factible incurrir en este error y que en ese momento no lo tengamos en cuenta y haga el ingreso en la cuenta fraudulenta. Además, es importante remarcar que los hackers son capaces en muchos casos de copiar la firma de correo del usuario, o crear un documento bancario con los datos del usuario, etc. Por lo que puede crear un perfil muy exacto para hacerse pasar por otra persona y esto ayuda a realizar el engaño.

Con el fin de evitar dicha situación y los peligros de la suplantación de identidad que ello conlleva, se deben adoptar todas las cautelas posibles, entre otras, las siguientes:

- Análisis periódico de los equipos en busca de nuevos virus informáticos.
- Protocolo de seguridad en el que NUNCA se atienda a un cambio de cuenta bancaria sin hablar antes personalmente con el cliente/proveedor propietario de esa cuenta.

- Revisión de filtros de correo (a nivel de servidor de correo) en vistas a que el hacker no haya puesto una redirección o respuesta automática (para que no nos lleguen los correos de un usuario y le reboten al propio hacker). Es decir, revisar que no tenemos filtros indeseados en el correo electrónico, sobre todo a nivel de correos corporativos.
- Tener una mínima duda de que la persona con la que estamos tratando pueda no ser realmente aquella con la que creemos interactuar, lo que nos hará estar en guardia en todas las situaciones en las que se vea afectados intereses económicos.

7.2 Virus informáticos

Los virus informáticos siguen siendo un problema fundamental tanto para empresas como para los usuarios particulares. Es imposible estar libre de la actuación de los virus, ni teniendo el antivirus más eficiente del mundo, por lo tanto, debemos ser conscientes del problema que esto supone y debemos tener en cuenta unas pautas de seguridad básicas para estar lo menos expuestos posible.

A continuación, indicamos algunos ejemplos de los principales virus informáticos de la actualidad, y en concreto, de aquellos más peligrosos y que más afectan a todo tipo de usuario:

- **Virus del correo electrónico**, que entra a través del correo de un cliente/proveedor conocido por GORONA. El hecho de recibir un correo de una persona conocida nos motiva a abrir el fichero adjunto que en realidad es un virus. El virus accede a nuestra bandeja de entrada de correo y se auto reenvía a todos nuestros contactos, motivando así su rápida propagación. Este virus no causa pérdida de datos, pero al enviarse a todos nuestros contactos empeora nuestra reputación. Al mismo tiempo, puede quedar latente a la espera de abrir puertas a nuevos virus o en el peor de los casos a encriptar los datos de nuestro equipo.

  Si abrimos un correo electrónico y/o un archivo adjunto del mismo y vemos que el archivo no se abre ni “hace nada”, debemos sospechar de dicho correo. Aunque parezca que no ha pasado nada, el virus estará actuando en segundo plano infectando y propagándose a nuestros contactos. Ante cualquier duda, debemos apagar el equipo o desconectarlo de Internet y solicitar ayuda inmediata a nuestro responsable o asesor informático.

- **Virus encriptado**, que puede acceder a nuestro sistema por varios procesos: Al hacer clic en un enlace de un email fraudulento, al entrar en páginas web dudosas y ejecutar algún programa que queremos descargar e instalar en nuestro equipo o de forma automática si tenemos puertos abiertos en el servidor, por ejemplo, para acceder desde fuera de la oficina de forma remota.

  Este virus causa una importante pérdida de datos. Se encriptan los archivos del ordenador donde entra y de todas las carpetas de la red a la que tiene acceso ese ordenador. Incluso las versiones más peligrosas se propagan por toda la red y pueden llegar a causar infecciones masivas de equipos. Al encriptar los archivos nos aparece un mensaje con una cuenta y un importe para recuperar dichos archivos.

  Para prevenir la ejecución de este tipo de archivos debemos seguir la norma de no abrir correos que no estamos seguros, nunca debemos descargar o instalar archivos de Internet que no estemos seguro de que son totalmente fiables, debemos minimizar la apertura de puertos externos en nuestro Reuter y por supuesto, debemos limitarnos a acceder a páginas seguras que tengan que ver con nuestro trabajo.

7.3 Programas basura

Son aquellos que se instalan en nuestro ordenador (en el propio sistema, en los navegadores, etc.) y ralentizan todo nuestro equipo e incluso toda nuestra red. Este tipo de programas tienen la misión de emitir publicidad, redirigir nuestras búsquedas a páginas de Internet nocivas, consumir recursos de nuestra red en beneficio propio.

No producen perdida de datos. Simplemente son programas que no sirven para nada y que consumen recursos y ralentizan y perjudican a nuestro sistema, pero si no controlamos su ejecución, podemos ver cómo van aumentando su incidencia en los equipos donde están instalados, hasta llegar al punto que no se puede trabajar con el equipo e incluso que rompe el propio sistema e impide que arranque con normalidad.

Para evitar la instalación de este tipo de programas no debemos nunca instalar programas por nuestra cuenta a no ser que seamos usuarios especializados y que tengamos la autorización del responsable informático de GORONA. Este tipo de programas se instalan muchas veces dentro de paquetes de instalación

de otros programas habituales que parecen “gratuitos”, pero que nos están instalando publicidad guiada en nuestro equipo de forma indirecta.

En el caso de que los programas ya estén instalados en nuestro equipo, hay que desinfectar tanto la instalación de programas del sistema (agregar o quitar programas), como la configuración de los navegadores (dentro del Chrome, Explorer, Firefox), ya que ahí también se instalan como complementos o plugin.

8 ACTUACIONES PREVENTIVAS

En definitiva, los aspectos a tener en cuenta para estar lo menos expuesto posible a virus, ataques y otras agresiones informáticas, en sus diversas versiones, serían al menos en estricto cumplimiento de las normas de seguridad siguientes:

- No abrir ningún correo electrónico que no ti tengamos claro su procedencia. En caso de abrir un correo electrónico para ver el contenido, si no conocemos al remitente, no pulsaremos en ningún enlace o no descargaremos ningún archivo adjunto.

- Desconfiar de los servicios de aviso de entidades oficiales (Correos, Hacienda, Seguridad Social, etc.) bancos o grandes empresas o similares. Antes de abrir cualquier correo electrónico de este tipo, aunque sea de una entidad conocida, debemos realizar un pequeño análisis de lo que nos están enviando. En caso de no tener clara su validez, intentar hablar con el remitente si eso es factible y confirmar y, sino, poner el asunto en el mano del experto informático.

- No entrar en el correo electrónico personal ni en redes sociales desde los equipos de la empresa, ya que son nichos en cuanto a la instalación de programas publicitarios en segundo plano.

- No entrar en páginas web marcadas como no seguras, y sobre todo no entrar en páginas web fraudulentas, de descargas, de contenidos online pirateados, etc.

- Comprobar enlaces. Si nos situamos encima de un enlace dentro de un correo, podemos ver donde apunta ese enlace. Desconfiemos de los enlaces de dominios o palabras extrañas.

- No descargar archivos ni programas no originales, ni instalar en los equipos programas propios sin el consentimiento del responsable de sistemas.

- Mantener un análisis periódico de los equipos en busca de nuevos virus informáticos.

- Avisar al responsable informático de una posible detección de virus, mal funcionamiento del equipo, lentitud extrema en algunos procesos y todo lo que pueda suponer la infección de un virus.

- En casos extremos, ante cualquier duda, apagar el equipo o desconectarlo de la red.

- Entrar solo a aquellas páginas web que necesitemos para desempeñar correctamente nuestro trabajo.

- Acceder a las páginas web marcadas como seguras (HTTPS). Dudar en caso contrario.

- No descargar ni ejecutar archivos de páginas web que desconozcamos.

- Identificar la localización y procedencia de la web donde queremos comprar Imprescindible entrar en páginas con certificado seguro HTTPS siempre que vamos a pagar.

- Utilizar métodos de pago seguros y establecidos que permitan reclamar: PAYPAL, pagos con tarjeta en pasarelas de pago de bancos conocidos por nosotros, contra reembolso, etc.

- Nunca bajo ningún concepto ofrecer o enviar nuestros datos de tarjeta de crédito a nadie, solo introduciremos dichos datos en formularios seguros de pasarelas de pago de bancos conocidos.

- El cambio periódico de contraseñas de cualquier sistema, y por supuesto del correo electrónico, siempre es beneficioso. Puede ser que nuestra contraseña haya sido descubierta por cualquier programa informático y si cambiamos la misma impediremos que sigan visualizando o accediendo a nuestros datos. Un cambio de contraseñas cada cuarenta y cinco días o, como máximo noventa, sería lo ideal.

- Los filtros de correo son unas herramientas que nos permiten crear respuestas automáticas, redirecciones, etc. Pero estas funciones también las aprovechan los hackers, por ejemplo, para entrar en conversaciones ajenas o recibir correos que van dirigidas a otras cuentas. Es importante que entremos en la configuración de estos filtros (nosotros o nuestro responsable informático) y revisemos de forma periódica que no hay ningún filtro nocivo o ajeno a nosotros. Esta revisión, también debe ser un protocolo periódico. En caso de no poder ser realizada por el usuario, deberá realizarse por el responsable de sistemas de GORONA.

- Los datos almacenados en nuestro ordenador deben de estar incluidos en la copia de seguridad de nuestro sistema. De no ser así, o incluimos estos datos en la copia de seguridad, o guardamos estos datos directamente en el servidor o en otra carpeta que esté dentro del sistema de copias. Lo que no puede ocurrir es que GORONA trabaje con un servidor y guardemos los datos en nuestro equipo (que es ajeno a cualquier tipo de copia), porque en ese caso, en caso de cualquier problema informático, podríamos perder toda la información del equipo.

- Los datos de GORONA que hay en nuestro equipo y los que tenemos acceso desde el mismo (a carpetas de la red), son datos muy importantes y los debemos tratar con el máximo cuidado. Debemos estar atentos al trabajar con dichos archivos, porque una mala acción puede provocar la perdida de información, con la pérdida de tiempo y dinero que ello supone.

- Cuando eliminamos un archivo de un ordenador, este pasa automáticamente a la “papelera”, pero cuando eliminamos un archivo del servidor desde un ordenador, este archivo se elimina directamente sin pasar por la papelera. Por eso hay que estar atento y trabajar con el máximo cuidado. Si ocurre esto, aun podemos recuperar el archivo desde el servidor o a través de la copia de seguridad, pero tenemos más posibilidad de pérdida de datos.

- El acceso a los datos por parte de un usuario a un servidor debe de estar limitado en función de las necesidades de cada trabajador. No tiene sentido, por ejemplo, que un técnico acceda a las carpetas de administración, o que un asesor acceda a las carpetas de dirección. Estos fallos de seguridad deben de ser informados al responsable de la informática, porque puede provocar grandes problemas a nivel interno de GORONA.

- El almacenamiento de datos en la nube es tendencia en los últimos años y son las bases del trabajo del futuro. Pero todavía es pronto para confiar plenamente en la nube, hay que ir con precaución. No por tener los datos en la nube estamos exentos de virus o de perdida de datos. Además, en caso de errores de Internet nos podemos ver sin acceso a los mismos, con todos los problemas que ello supone. Por lo tanto, es importante prevenir estas situaciones también. Debemos tener copia de seguridad "en local", para evitar pérdidas de datos en el propio proveedor que ofrece el servicio, así como poder trabajar en momentos puntuales en los que haya perdida de conexión a Internet.

- Debemos conocer que sistema de datos en la nube tenemos contratado. No es lo mismo un servicio plano de almacenamiento, donde podemos tener un virus y que este se propague a la nube y perderlo todo; a tener un sistema de datos con copias de seguridad automáticas y distintas versiones, que nos permita restablecer directamente los datos en caso de propagación de virus.

- Si vamos a realizar el pago de una factura a un proveedor nuestro debemos asegurarnos al 100% de que la cuenta donde se va a realizar el ingreso es la correcta. En cuentas que ya hemos utilizado en anteriores ocasiones ya tenemos la certeza de que esto ocurre, pero en cuantas nuevas o cuentas que modifican los clientes, hay que asegurarse personalmente de que este cambio es correcto.

- Lo mismo ocurre para aquellos cobros que estamos esperando de clientes. Debemos avisar que GORONA no cambiará nunca el número de cuenta donde se deben realizar los ingresos, salvo comunicación expresa de la persona responsable realizada de forma que no ofrezca ninguna duda de su personalidad.

- En cualquier transacción debemos asegurar que los números de cuenta son correctos, porque si realizamos transferencias a cuentas erróneas que están controladas por hackers, el dinero desaparece rápidamente y es muy difícil recuperarlo.

- Todos los ordenadores deben de tener el antivirus correctamente instalado y configurado. Los antivirus analizan de forma continua toda la actividad del equipo, pero es importante que de forma periódica se realice un análisis completo de todos los equipos. Este análisis debe obtener los resultados

esperados (equipo limpio y sin problemas). De no ser así, se deben revisar los resultados y ante la duda indicarlo al responsable o asesor informático.

- En algunas ocasiones, no es obligatorio, pero si muy recomendable, que los ordenadores cuenten con un programa antimalware, que complemente al antivirus y ayude a resolver los problemas y restos de virus que este no pueda limpiar. Estos programas (habitualmente son gratuitos, como por ejemplo el programa Malware bytes) permiten encontrar restos de virus que los propios antivirus consideran como “buenos”. De esta manera atacamos las amenazas desde dos puntos de vista y por lo tanto mejoramos la seguridad de nuestro sistema.

- Las actualizaciones de Windows y de los programas que usamos en nuestro día a día son muy importantes. En gran medida, las actualizaciones se centran en cubrir fallos de seguridad, que a priori parecen poco importantes, pero que realmente son los “agujeros” que utilizan los virus para acceder a nuestros sistemas.

- Realización sistemática y automatizada de copias de seguridad, que deben estar bien configuradas y ser supervisadas periódicamente para comprobar que se ejecutan según el plan previsto y la integridad de los archivos.

- Establecer protocolos para no conectar dispositivos de almacenamiento externo por parte de los trabajadores, no conectar cuentas de correo electrónico personales, no instalar programas de archivos en la nube, etc.

ANEXO I: ESQUEMA DE GESTIÓN DE ACCESOS Y SISTEMA DE IDENTIFICACIÓN.

PROTOCOLO DE SEGURIDAD INFORMÁTICA GORONA DEL VIENTO EL HIERRO, S.A.

POLÍTICA DE ACCESO

Objetivo:
Garantizar que solo las personas autorizadas tengan acceso a los sistemas y datos de la organización.

Responsabilidades:
La dirección de GORONA es responsable de aprobar y revisar la política de acceso.
El equipo de seguridad de la información bajo la dirección de la Secretaría General Técnica es responsable de implementar y hacer cumplir la política.
Todos los empleados y contratistas deben cumplir con la política de acceso.

IDENTIFICACIÓN Y AUTENTICACIÓN

Identificación:
Cada empleado y usuario autorizado debe tener una identificación única, como un nombre de usuario o un número de empleado.

Autenticación:
Se requiere autenticación de dos factores (2FA) para acceder a sistemas y datos sensibles.
Los métodos de autenticación pueden incluir contraseñas, tarjetas inteligentes, huellas dactilares o autenticación biométrica.

CONTROL DE ACCESO

Políticas de Control de Acceso:
Se deben definir las políticas de acceso basadas en roles para determinar qué recursos y datos pueden acceder los usuarios en función de sus funciones y responsabilidades.

Privilegios Mínimos:
Los usuarios deben tener los privilegios mínimos necesarios para realizar sus tareas laborales.
Se deben implementar controles para garantizar que los usuarios no tengan más acceso del necesario.

AUDITORÍA Y MONITOREO

Registro de Auditoría:
Se debe habilitar la auditoría de accesos para registrar todas las actividades de los usuarios, incluidos los intentos de acceso no autorizados.

Monitoreo Continuo:
Se debe realizar un monitoreo continuo de los registros de auditoría para detectar y responder a actividades sospechosas o no autorizadas.

GESTIÓN DE CONTRASEÑAS
Ver Anexo V Política de Contraseñas.

PROCESO DE SOLICITUD DE ACCESO
Ver Anexo II Solicitud de nuevo usuario y Anexo IV Orden acceso a terceros.

RESPUESTA A INCIDENTES DE ACCESO NO AUTORIZADO

Procedimientos de Respuesta:
Se deben establecer procedimientos de respuesta a incidentes para abordar situaciones de acceso no autorizado.

Investigación y Mitigación:
Cualquier incidente de acceso no autorizado debe investigarse, mitigarse y documentarse adecuadamente.
Para más información consultar el Anexo VI Plan de Gestión de Incidentes de Seguridad de la Información.

ANEXO II: SOLICITUD DE NUEVO USUARIO.

PROTOCOLO DE SEGURIDAD INFORMÁTICA GORONA DEL VIENTO EL HIERRO, S.A.

SOLICITUD DE NUEVO USUARIO	
Solicitante:	**Fecha:**
Datos del nuevo usuario: - Nombre Completo: [Nombre del Nuevo Usuario] - Departamento: [Departamento del Nuevo Usuario] - Cargo: [Cargo del Nuevo Usuario] - Fecha de Inicio: [Fecha de Inicio del Nuevo Usuario]	
Recursos y acceso requeridos: - [Lista de Sistemas o Datos a los que se Requiere Acceso] - [Privilegios Específicos, si corresponde]	
Justificación: Justificación de la solicitud de nuevo usuario.	
Peticionario: Fdo. *(firmado electrónicamente)* (Puesto)	Aprobado por: Fdo. *(firmado electrónicamente)* (Secretaría General Técnica)

ANEXO III: NOTIFICACIÓN DE REVOCACIÓN DE ACCESO.

PROTOCOLO DE SEGURIDAD INFORMÁTICA GORONA DEL VIENTO EL HIERRO, S.A.

REVOCACIÓN DE ACCESO	
Fecha	**Usuario:**
Motivo de la revocación: [Motivo de la Revocación, por ejemplo, término de empleo]**	
Acceso revocado a los siguientes recursos: - [Lista de Sistemas o Datos a los que se Revocará el Acceso]	
Acción requerida: Se notifica a [Nombre del Usuario] que su acceso a los recursos mencionados ha sido revocado a partir de [Fecha de Revocación]. Debe devolver todos los dispositivos, contraseñas y credenciales de acceso de inmediato.	
Firma de confirmación: Fdo. *(firmado electrónicamente)* (Puesto)	Recibí: Fdo. *(firmado electrónicamente)* (Secretaría General Técnica)

ANEXO IV: ORDEN DE ACCESO A TERCEROS.

PROTOCOLO DE SEGURIDAD INFORMÁTICA GORONA DEL VIENTO EL HIERRO, S.A.

ORDEN DE ACCESO A TERCEROS	
Fecha	**Proveedor/contratista:**
Objetivo: La siguiente orden autoriza a [Nombre del Proveedor/Contratista] a acceder a los sistemas y datos de [Nombre de la Empresa] con el propósito de [Especificar el Propósito, por ejemplo, mantenimiento de sistemas].	
Detalle de acceso autorizado: - Período de Acceso: [Fecha de Inicio] - [Fecha de Finalización] - Recursos de Acceso: [Lista de Sistemas o Datos a los que se Accederá] - Responsable del Acceso: [Nombre y Cargo del Responsable Interno]	
Responsabilidades: - [Nombre del Proveedor/Contratista] es responsable de cumplir con todas las políticas de seguridad de la información de [Nombre de la Empresa]. - [Nombre del Proveedor/Contratista] no debe divulgar, copiar o utilizar información confidencial sin autorización. - [Nombre del Proveedor/Contratista] debe informar cualquier incidente de seguridad o incumplimiento de la política de seguridad de inmediato a [Responsable Interno]. - [Nombre del Proveedor/Contratista] debe seguir todas las reglas y regulaciones aplicables durante el acceso.	
Firma del representante de terceros: Fdo. [Nombre] *(firmado electrónicamente)* (Cargo)	Aprobado por: Fdo. [Responsable interno] *(firmado electrónicamente)* (Cargo)

ANEXO V: POLÍTICA DE GESTIÓN DE CONTRASEÑAS.

PROTOCOLO DE SEGURIDAD INFORMÁTICA GORONA DEL VIENTO EL HIERRO, S.A.

Fecha de Vigencia: [Fecha de Vigencia]

Objetivo:
Esta política tiene como objetivo garantizar el uso seguro y eficaz de contraseñas para proteger la información de la empresa.
Responsabilidades:
- Todos los empleados y contratistas deben cumplir con esta política.
- El equipo de seguridad informática es responsable de hacer cumplir esta política.

Requisitos:
1. La conexión de usuarios con la red local de Gorona del Viento El Hierro, S.A. se apoyará un Active Directoy o Azure Active Directory que obligan al cumplimiento de ciertos requisitos. En todos los casos se contemplarán los aspectos más relevantes como:
    a. periodos de validez para las contraseñas: permanente.
    b. posibilidad de reutilización de contraseñas ya usadas: se admite.
    c. formato de la contraseña: longitud mínima; tipos de caracteres que deben incluir; cumplimiento de reglas semánticas.
    d. posibilidad de elección y modificación de la contraseña por parte del usuario: no permitido.
    e. almacenamiento de las claves: tamaño del histórico de claves a almacenar para cada usuario; método de encriptación de las claves.
    f. número de intentos de autenticación permitidos.
2. No utilizar las contraseñas por defecto. Esto es especialmente importante para el acceso a la configuración de ciertos dispositivos como routers, switches, etc.
3. Doble factor para servicios críticos:
    a. Acceso al gestor de expediente “Gestiona”.
    b. Acceso al administrador de Microsoft 365.
    c. Instalación de software de Microsoft 365 a nivel usuario.
    d. Aquellos servicios o aplicaciones críticas a las que no pueda aplicarse el doble factor serán modificadas periódicamente.
4. No compartir las contraseñas:
    a. no debemos compartirlas con nadie ni mencionarla en conversaciones o comunicaciones de cualquier tipo;
    b. no debemos apuntarlas en papeles o post-it;
    c. no debemos escribir nuestras contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.
    d. no enviar nunca la contraseña por redes sociales o en un SMS.
5. Las contraseñas deben de ser robustas, debemos cumplir las siguientes directrices:
    a. deben contener al menos ocho caracteres;

   b. deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);
   c. no deben contener los siguientes tipos de palabras: palabras sencillas en cualquier idioma (palabras de diccionarios); nombres propios, fechas, lugares o datos de carácter personal; palabras que estén formadas por caracteres próximos en el teclado; palabras excesivamente cortas.
   d. tampoco utilizaremos claves formadas únicamente por elementos o palabras que puedan se públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento);
   e. se establecerán contraseñas más fuertes para el acceso a aquellos servicios o aplicaciones más críticas;
   f. se tendrá en cuenta lo expuesto en los puntos anteriores también en el caso de utilizar contraseñas de tipo passphrase (contraseña larga formada por una secuencia de palabras).
6. No utilizar la misma contraseña para servicios diferentes.
7. No hacer uso del recordatorio de contraseñas.
8. Se prohíben técnica de autentificación basadas en la utilización de identidades ya creadas en redes sociales (como Facebook, Linkedin, Google o Twitter) para registrarnos automáticamente en otros servicios.
9. Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de estas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
10. Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
11. Cifrar las que se generen en las diferentes aplicaciones que deban viajar por la red.
12. No utilizar en ningún caso las que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
13. No escribirlas en equipos de cómputo de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
14. Informar cualquier incidente de seguridad que ponga en riesgo su contraseña a la SGT.
15. Informar a la SGT si alguien dentro o fuera de la entidad se la solicita.
16. No permitir que le observen al escribirla.

Detalles sobre las medidas de seguridad para el almacenamiento de contraseñas:

Las contraseñas de usuarios generales (no personales) serán archivadas en el gestor de expedientes con carácter CONFIDENCIAL cuyo acceso lo tienen la Secretaría General Técnica y en quien delegue.

ANEXO VI: PLAN DE GESTIÓN DE INCIDENTES.

PROTOCOLO DE SEGURIDAD INFORMÁTICA GORONA DEL VIENTO EL HIERRO, S.A.

Fecha de Vigencia: [Fecha de Vigencia]

Objetivo:
Este plan tiene como objetivo proporcionar una guía para la detección, notificación y respuesta eficaz a incidentes de seguridad de la información.

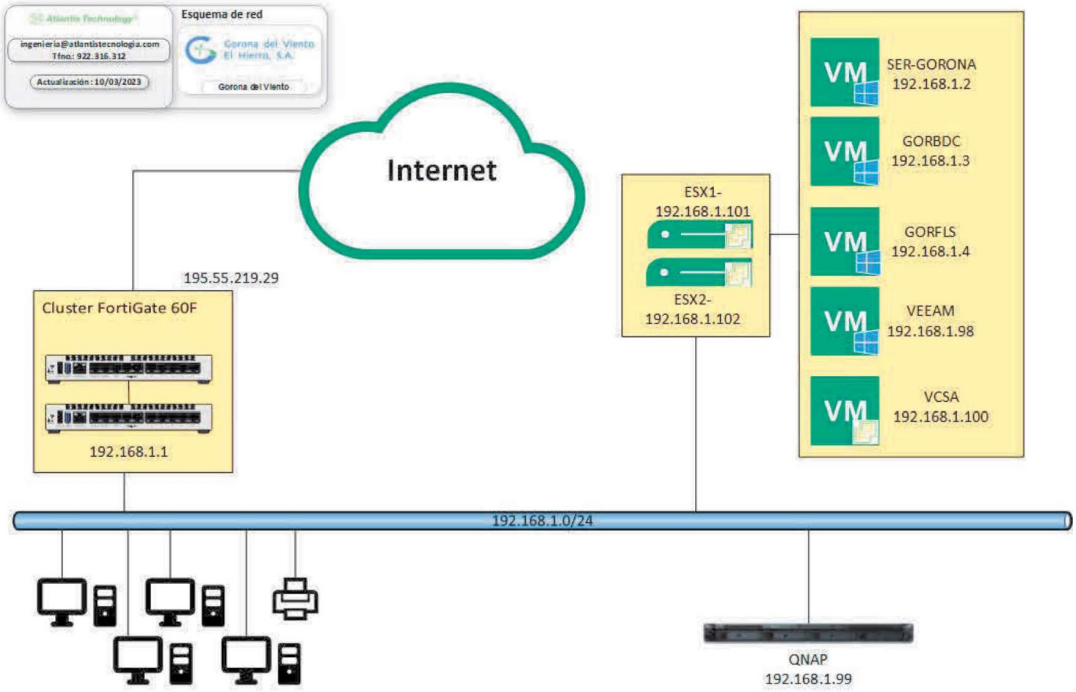
Responsabilidades:
- El equipo de seguridad de la información bajo la dirección de la Secretaría General Técnica es responsable de coordinar y gestionar los incidentes de seguridad.

- Todos los empleados deben informar de inmediato cualquier incidente de seguridad sospechoso o confirmado.

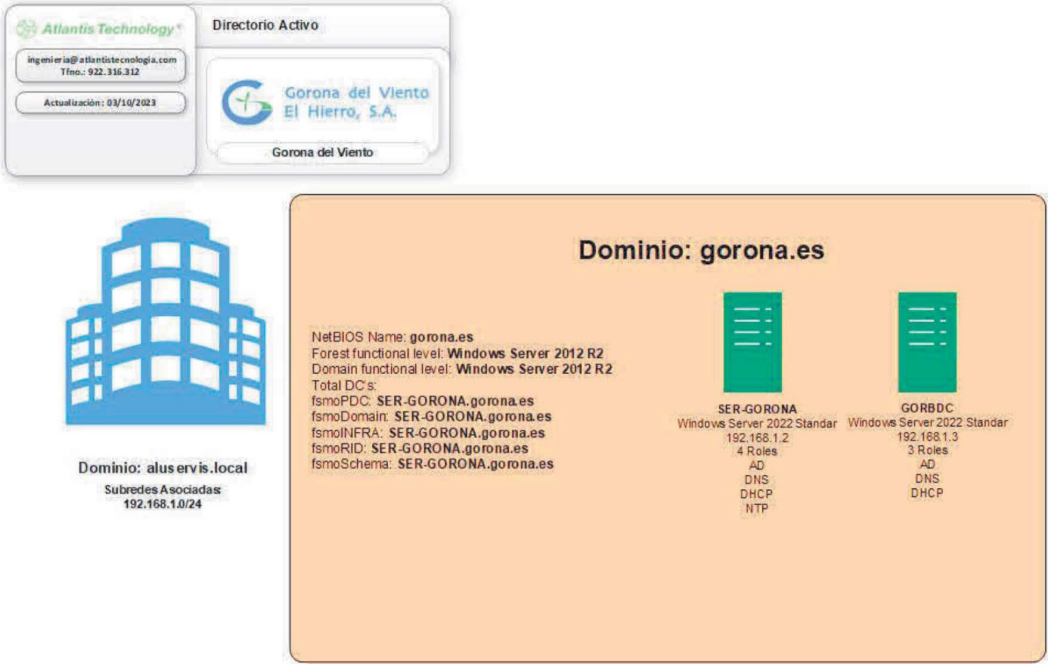
Esquema de actuación ante un incidente:
Se anexan Esquemas.

7. Esquemas

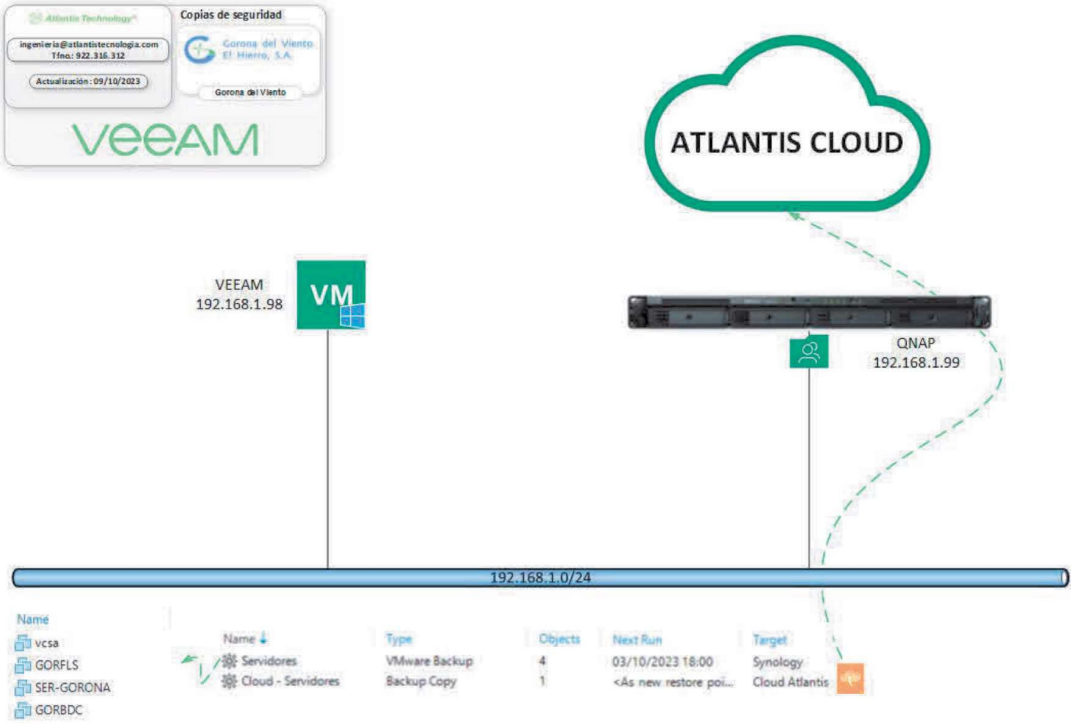
7.1 Esquema de red



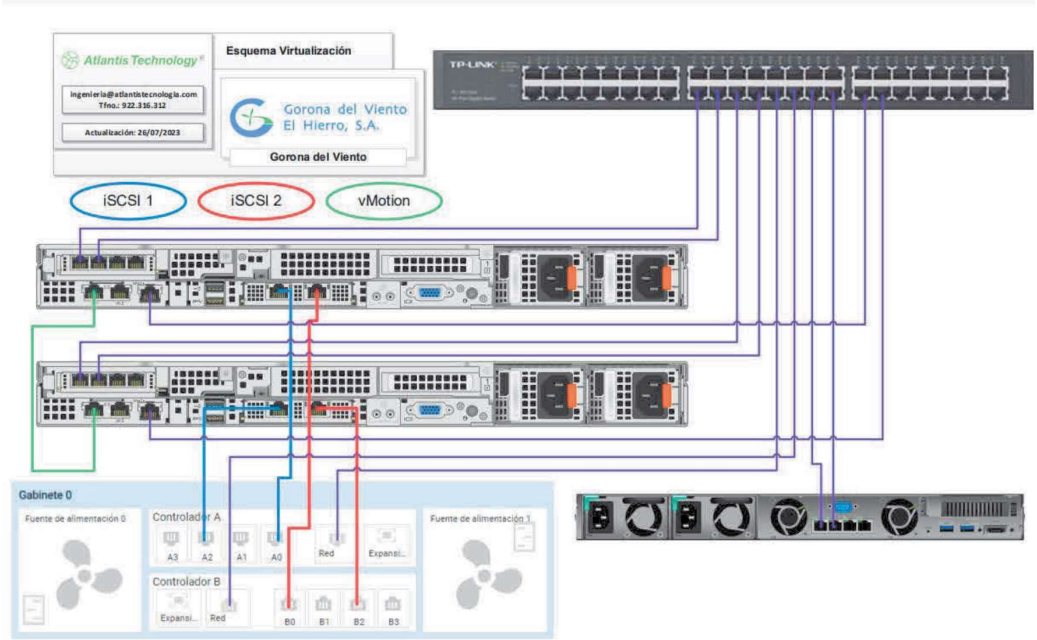
7.2 Esquema AD



7.3 Esquema copias de seguridad



7.4 Esquema Virtualización



ANEXO VII: PROCEDIMIENTO DE INSTALACIÓN DE SOFTWARE Y SEGURIDAD DE LA INFORMACIÓN.

PROTOCOLO DE SEGURIDAD INFORMÁTICA GORONA DEL VIENTO EL HIERRO, S.A.

Objetivo:

Este procedimiento tiene como objetivo garantizar que la instalación de software en la empresa se realice de manera segura y cumpla con las leyes y regulaciones relacionadas con el uso de software.

Responsabilidades:

1. Personal designado como IT:
    a. Supervisar y coordinar el proceso de instalación de software.
    b. Validar la licencia y la legalidad de todo el software adquirido o utilizado en la empresa.
2. Equipo de seguridad informática bajo la dirección de la Secretaria General Técnica:
    a. Revisar y aprobar cualquier solicitud de instalación de software.
    b. Evaluar los riesgos de seguridad asociados con el nuevo software.
3. Empleados:
    a. Solicitar autorización para la instalación de software siguiendo este procedimiento.
    b. Cumplir con todas las políticas de seguridad de software y las leyes de derechos de autor.

Solicitud de Instalación de Software:

Los empleados que requieran la instalación de software deben completar un formulario de solicitud de instalación de software que incluya la siguiente información:

- Nombre del software.
- Propósito de la instalación.
- Justificación comercial.
- Fecha de instalación deseada.

La solicitud debe ser aprobada por la Secretaría General Técnica o Responsable designado por esta.

Evaluación de Riesgos y Aprobación:

El equipo de Seguridad Informática evaluará los riesgos de seguridad asociados con la instalación propuesta y determinará si es segura y legal.

Si se aprueba la solicitud, se asignará al personal técnico de IT (interno o externo, según necesidades del servicio) para llevar a cabo la instalación siguiendo las mejores prácticas de seguridad.

Verificación de Legalidad del Software:

Antes de proceder con la instalación, se verificará la legalidad del software:

- Se comprobará que se dispone de una licencia válida para el software.
- Se verificará que el software proviene de una fuente legítima y de confianza.

Instalación y Configuración:

La instalación y configuración del software se llevarán a cabo por personal autorizado de IT siguiendo las directrices del fabricante y las mejores prácticas de seguridad.

Registro y Documentación:

Se mantendrá un registro de todas las instalaciones de software, incluyendo detalles como el nombre del software, la fecha de instalación, el responsable y el propósito.

Capacitación de Usuarios:

Los usuarios finales que utilizarán el software deberán recibir capacitación sobre su uso seguro y las políticas de seguridad relacionadas.

Cumplimiento y Auditoría:

Se realizarán auditorías periódicas para verificar el cumplimiento de este procedimiento y para asegurarse de que no se esté utilizando software ilegal o no autorizado.

Eliminación Segura:

Cuando un software ya no sea necesario, se debe eliminar de manera segura para evitar posibles riesgos de seguridad.

Sanciones:

El incumplimiento de este procedimiento puede resultar en medidas disciplinarias, incluida la terminación del empleo.

---------- 000 ----------