

ACUERDO DE CONEXIÓN DE USUARIO DE NOAA NET

SECCIÓN 1 – REEMPLAZA

Ningún acuerdo.

SECCIÓN 2 - INTRODUCCIÓN

Este Acuerdo de Conexión de Usuario de NOAA net (*NOAA net User Connection Agreement*, NUCA, en adelante el Acuerdo de Conexión) autoriza y documenta el entendimiento, los roles y las responsabilidades entre la red de área amplia (*Wide Area Network*, WAN) NOAA net (NOAA8204) del Servicio Nacional de Meteorología (*National Weather Service*, NWS), el Sistema Internacional de Comunicaciones por Satélite (*International Satellite Communications System*, ISCS) y el Usuario. Este acuerdo entre el NWS de la Administración Nacional Oceánica y Atmosférica (*National Oceanic and Atmospheric Administration*, NOAA) de EE.UU. y _____ el Usuario se establece para facilitar el desarrollo, la administración, la operación y la seguridad de una conexión entre ambas partes. Este acuerdo regirá la relación entre el NWS y el Usuario, incluyendo el personal administrativo y técnico designado a falta de una autoridad administrativa común. Este acuerdo entrará en vigor una vez firmado por el NWS y el Usuario.

SECCIÓN 3 - PROPÓSITO

El propósito del presente Acuerdo de Conexión es facilitar el compromiso del NWS para brindar acceso (datos de vuelta) con el fin de que los países que integran la Red Regional de Telecomunicaciones Meteorológicas (RRTM) puedan acceder al Sistema Mundial de Telecomunicaciones (SMT).

SECCIÓN 4 - DECLARACIÓN DE INTERÉS Y BENEFICIOS MUTUOS

El interés y los beneficios mutuos de esta conexión consisten únicamente en mantener el acceso al STM para los países miembros dentro de la RRTM de la Región IV.

SECCIÓN 5 - DESCRIPCIÓN GENERAL

NOAA net (NOAA8204) del NWS es una red compartida para propósitos generales que emplea servicios de conmutación de etiquetas multiprotocolo (*Multiprotocol Label Switching*, MPLS) para brindar una red troncal de WAN segura y privada. El sistema NOAA net comprende los dispositivos de nodo final, los routers y cortafuegos del nodo final del cliente (*Customer Edge*, CE); la WAN proporcionada por la portadora que conecta dichos dispositivos; un subsistema seguro fuera de banda para acceder y administrar sitios remotos en caso de una interrupción de la red; y los sistemas automatizados que administran y supervisan el tráfico entre los routers de nodo final del cliente.

NOAA net (NOAA 8204) fue designado como sistema de alto impacto y ejecuta los controles de seguridad necesarios para sistemas de alto impacto con base en requisitos de alta disponibilidad.

La información manejada por NOAA net (NOAA8204) del NWS tiene una clasificación de confidencialidad moderada. El nivel de clasificación de la información que se intercambiará es el de material no clasificado.

No se produce ningún intercambio de datos, es decir, el Usuario no transmite ni recibe datos de NOAA net y no se almacenan datos del Usuario dentro de los límites de NOAA net.

Servicios de datos

NOAAnet (NOAA8204) brinda servicios de cortafuegos y red privada virtual (*Virtual Private Network*, VPN) a través del acceso WAN de alta disponibilidad, cuando sea necesario, utilizado para conectar varios sistemas dentro del NWS y el Usuario. El propósito de estos servicios es facilitar el movimiento de datos a varios sistemas y desde ellos a través de internet por la conexión proporcionada por NOAAnet.

La pasarela (*gateway*) opera un agrupamiento de servidores que diseminan y reciben los archivos que contienen los datos meteorológicos en formatos predefinidos. El propósito de esta conexión es asimilar y difundir los datos. En términos generales, estos servicios de información (asimilación de datos) se caracterizan por:

- asimilación de archivos mediante SCP, HTTP y FTP;
- asimilación de mensajes, basados y no basados en protocolo de internet (IP), usando el protocolo X.25 o comunicaciones asíncronas.

Responsabilidades de registro de auditoría

Los dispositivos de nodo final de NOAAnet están configurados para registrar todas las sesiones y todos los intentos de acceso fracasados. Los registros se comprimen, se archivan mensualmente y se conservan por un año. Los registros incluyen el tipo, la fecha y la hora del evento. El servicio NOAAnet (NOAA8204) del NWS requiere información de registro de auditoría del Usuario y no accede a los datos de auditoría a través de la conexión.

SECCIÓN 6 - COMUNICACIONES

Es esencial mantener comunicaciones formales frecuentes para asegurar la administración y operación correcta de la conexión. El NWS y el Usuario se comprometen a mantener líneas de comunicación abiertas entre el personal designado tanto a nivel administrativo como técnico. Todas las comunicaciones descritas en este documento deberán realizarse por escrito, a menos que se indique lo contrario.

El NWS y el Usuario convienen en designar líderes técnicos para sus respectivos sistemas (Apéndice A) y proporcionar información de contacto para ellos, así como facilitar el contacto directo entre los líderes técnicos para apoyar la administración y operación de la conexión. Para asegurar la confidencialidad, integridad y disponibilidad de los sistemas conectados y los datos que almacenan, procesan y transmiten, el NWS y el Usuario convienen en notificar sobre eventos específicos dentro de los plazos indicados abajo:

Comunidad de usuarios

Los datos y productos de la red NOAAnet (NOAA8204) del NWS forman una base de datos y una infraestructura nacional de información que otras agencias gubernamentales, el sector privado, el público y la comunidad mundial pueden utilizar.

Seguridad de intercambio de información

Todos los límites del servicio NOAAnet están bajo la vigilancia y protección de cortafuegos con control de estado. La norma de NOAAnet obliga el cumplimiento con servicios de cortafuegos con control de estado para todas las sesiones y en todos los dispositivos de nodo final administrados centralmente. El cortafuegos permitirá el acceso con base en:

1. dirección IP de origen
2. dirección IP de destino

3. protocolo (TCP/UDP)
4. puertos

El NWS utiliza directivas de cortafuegos basadas en el host para aplicar medidas de seguridad adicionales. Aunque el servicio NOAAnet (NOAA8204) no cifra los datos del cliente que pasan por la red, todo acceso a los dispositivos de nodo final de NOAAnet, ya sea a través de la red o mediante acceso externo (telefónico), requiere autenticación RSA de dos factores y se cifra en conformidad con FIPS140-2.

Expectativas de comportamiento confiable

Este apartado describe las expectativas en lo referente a las reglas de comportamiento que el servicio NOAAnet (NOAA8204) del NWS y el Usuario seguirán para proteger la información que estará expuesta a esta conexión. El NWS se reserva el derecho de finalizar este acuerdo si el Usuario no cumple con dichas expectativas.

- Los empleados y contratistas de NOAA se comprometen a seguir las pautas establecidas de acuerdo con las reglas de comportamiento de NOAA.
- El servicio NOAAnet (NOAA8204) del NWS espera que el Usuario siga los procedimientos de notificación y escalamiento descritos en este documento.
- El servicio NOAAnet (NOAA8204) del NWS espera que el Usuario tome medidas adecuadas para prevenir ataques operacionales, tales como los ataques de denegación de servicio.

Parámetros de seguridad

El acceso a los recursos y sistemas de la red de NOAA a través del enlace troncal NOAAnet se controla mediante servicios de cortafuegos con control de estado de NOAAnet en cada nodo final y se autentica con base tanto en el protocolo como en el puerto. NOAAnet proporciona y administra las conexiones de VPN y de cortafuegos según resulte necesario para asegurar la transferencia segura de los datos entre los sistemas del NWS y del Usuario. Todo cambio efectuado en el cortafuegos se somete a la dirección de control de cambios (*Change Control Board*, CCB) de NOAAnet para análisis y aprobación antes de su implementación.

Cambios materiales a la configuración del sistema

Los cambios técnicos previstos en la arquitectura del sistema en lo referente a la conexión se comunicarán al personal técnico antes de su implementación. El NWS se compromete a conducir un estudio de evaluación de riesgos con base en la nueva arquitectura del sistema y modificar y volver a firmar el Acuerdo de Conexión dentro de un (1) mes de dicha implementación.

Nuevas conexiones

El presente Acuerdo de Conexión NO AUTORIZA el establecimiento de nuevas conexiones a NOAAnet ni a otro sistema de TI, incluyendo los sistemas que pertenecen y son administrados por terceros.

Cambios de personal

El NWS y el Usuario convienen en informarse mutuamente cuando el propietario o líder técnico del sistema deje de trabajar en la organización o se ausente por un período prolongado. Además, ambas partes se mantendrán mutuamente informadas de cualquier cambio que ocurra en cuanto a la persona de contacto.

Procedimientos de notificación y escalamiento

En la eventualidad de que se produzca la interrupción o degradación del servicio, los usuarios deben notificar al Centro de Operaciones de la Red (*Network Operations Center, NOC*) de NOAA net llamando por teléfono al 1.888.NOAANET (1.888.662.2638) o enviando un mensaje por correo electrónico a noaanet.support@noaa.gov. Todos los usuarios de NOAA net deben proporcionar información de contacto (teléfono y dirección de email) en el reglón con la firma de sus mensajes relacionados con todo asunto de interrupción del servicio o de seguridad.

Entrenamiento y concientización

Todo el personal y los contratistas de NOAA deben terminar con éxito el programa de concientización de seguridad informática antes de que se autorice su acceso a los sistemas de información de NOAA/NWS, siempre que lo requieran los cambios del sistema y por lo menos una vez al año después de eso. Es posible que se conceda al Usuario acceso temporal al sistema si recibe una orientación sobre la seguridad del sistema de información como parte del dicho acceso, hasta que se satisfaga requisito de entrenamiento. En estos casos, el requisito de entrenamiento se deberá satisfacer dentro de un plazo de treinta (30) días de calendario. Si el Usuario se niega o no puede satisfacer el requisito de entrenamiento debido a circunstancias de fuerza mayor, el acceso a la información y los recursos se deberán suspender.

Corresponde al Director del Sistema de Tecnología de la Información (*Information Technology System Officer*) identificar todo entrenamiento de seguridad informática; el progreso del entrenamiento se sigue en el sistema de entrenamiento de concientización de seguridad informática de NOAA y se comunica a la Oficina de Seguridad Informática (*IT Security Office*) de NOAA y al Director de Tecnologías de la Información (*Chief Information Officer, CIO*) de NOAA.

El requisito de entrenamiento y concientización de seguridad informática no se extiende a la comunidad de usuarios del ISCS.

SECCIÓN 7 – SERVICIOS

Los servicios de NOAA net (NOAA8204) incluyen:

- desarrollo de una solución de diseño de la red;
- servicios de adquisición para hardware y servicios de telecomunicación;
- administración de logística, que incluye ordenar, coordinar la instalación y administrar en forma continua los servicios de portadora de telecomunicaciones;
- administración de equipos y configuración para todos los dispositivos de infraestructura administrados por NOAA net;
- garantía de servicios, lo cual incluye la administración de incidentes y problemas; y
- administración del rendimiento del sistema.

Modo operacional de seguridad

El Estándar Federal de Procesamiento de la Información (*Federal Information Processing Standard, FIPS*) 199 define las categorías de seguridad, los objetivos de seguridad para integridad, confidencialidad y disponibilidad, y los niveles de impacto bajo, moderado y alto. La selección de la categoría de seguridad de NOAA net (NOAA8204) se basa en la misión y:

- la pérdida confidencialidad (acceso no autorizado)
- la pérdida de integridad (modificación o destrucción no autorizados)
- la pérdida de disponibilidad (interrupción de acceso o uso)

SÓLO PARA USO OFICIAL

La clasificación de seguridad (*Security Categorization, SC*) de NOAAnet (NOAA8204) se ha establecido usando como guía el estándar FIPS 199 y la publicación especial del Instituto Nacional de Normas y Tecnología (*National Institute of Standards and Technology, NIST*) denominada (SP) 800-60. El proceso y el análisis se documentan en la norma FIPS 199 SC de NOAAnet (NOAA8204) mientras que dicho sistema NOAAnet (NOAA8204) del NWS apoye la clasificación de seguridad siguiente para confidencialidad, integridad y disponibilidad de los datos transmitidos a través de esta conexión:

SC NOAA8204 = {(confidencialidad, moderada), (integridad, moderada), (disponibilidad, alta)}

Nivel de impacto del sistema de información (para selección de controles de línea de base):
impacto ALTO

- confidencialidad: moderada
- integridad: moderada
- disponibilidad: alta

Restricciones específicas del equipo

La comunidad de usuarios del ISCS que se conecta a la WAN NOAAnet del NWS debería poder establecer la conexión por Ethernet o fibra.

Documentación de seguridad

El NWS y NOAAnet operan de acuerdo con planes de seguridad del sistema que satisfacen los requisitos descritos en la publicación especial SP 800-53, rev. 2 de NIST. El NWS opera NOAAnet (NOAA8204) bajo las pautas de seguridad de NIST para certificación y acreditación (C&A). La certificación y acreditación de NOAAnet está cubierta por el sistema NOAA8204 que recibió su autoridad para funcionar (*Authority to Operate, ATO*) en diciembre de 2008.

SECCIÓN 8 – RESPONSABILIDADES

Responsabilidades de la oficina del CIO del NWS

La oficina del CIO del NWS es responsable de establecer y apoyar los servicios NOAAnet en conformidad con los términos del acuerdo de nivel de servicio (*Service Level Agreement, SLA*) de NOAAnet.

Responsabilidades de la oficina del programa ISCS

Especificar los puntos de contacto para notificación en caso de interrupción del servicio o de eventos planeados que puedan afectar la entrega de los servicios.

Responsabilidades de la comunidad de usuarios de NOAAnet

- Recibir y aceptar los servicios de forma oportuna;
- determinar y comunicar los requisitos del cliente;
- asumir responsabilidad por equipos perdidos o robados;
- seguir los procedimientos de notificación y escalamiento de NOAAnet;
- verificar y acusar recibo de todo equipo y periférico proporcionado por el ISRC;
- aceptar propiedad y responsabilidad de administración para todo el ciclo de vida del producto para todo equipo y periféricos proporcionados por el ISRC.

SECCIÓN 9 – POLÍTICA FORMAL DE SEGURIDAD

El servicio NOAAnet (NOAA8204) del NWS se rige por las políticas de seguridad de la información del gobierno federal de Estados Unidos, como las de la Oficina de Gestión y

SÓLO PARA USO OFICIAL

10/8/2009

5 de 10

Presupuesto (*Office of Management and Budget, OMB*), del Departamento de Comercio (*Department of Commerce, DOC*) y de NOAA. Encontrará más detalles en la página 24 del plan de seguridad del sistema SSP de NOAAnet, v1.4 del 8 de diciembre del 2008.

SECCIÓN 10 - DESASTRES Y OTRAS CONTINGENCIAS

En caso de desastre, el NWS seguirá el plan de contingencia (*Contingency Plan, CP*) de NOAAnet. Dicho plan establece procedimientos para la recuperación del sistema de información después de una interrupción del servicio. Se han establecido los siguientes objetivos para este plan:

- Identificar las fases siguientes:
 - o Notificación/activación: detectar y determinar el daño y activar el plan.
 - o Restauración: brindar operaciones informáticas temporales y/o recuperarse del daño que sufrió el sistema original hasta que se alcance un nivel que permita apoyar el sistema y los procesos del ISCS.
 - o Reconstitución: restaurar las operaciones normales del ISCS.
- Identificar las actividades, los recursos y los procedimientos necesarios para llevar a cabo los requisitos identificados del sistema durante una interrupción prolongada de las operaciones normales.
- Asignar responsabilidades al personal designado del NWS y los contratistas para brindar la dirección necesaria para lograr la recuperación del sistema del ISCS durante períodos prolongados de interrupción de las operaciones normales.
- Asegurar la coordinación con otro personal del NWS y los puntos de contacto externos que participan en las estrategias de planificación para situaciones de emergencia.

SECCIÓN 11 - LÍMITES DEL SISTEMA Y DISPOSICIÓN FÍSICA

La oficina del CIO del NWS es responsable de apoyar y administrar los equipos asociados al router del nodo final del cliente (*Customer Edge, CE*) y todo equipo relacionado empleado para medir el rendimiento y las comunicaciones fuera de banda, incluyendo sondas y módems. Todas las oficinas cuentan con una solución de acceso directo al enlace troncal de NOAAnet. Toda la actividad de ingreso y salida se captura en registros de auditoría del router del nodo final del cliente.

SECCIÓN 12 - MODIFICACIÓN, TERMINACIÓN, Y OTRAS CONDICIONES

El NWS podrá modificar el Acuerdo de Conexión previa notificación del Usuario en un plazo razonable. El NWS o el Usuario podrá terminar su participación en el Acuerdo de Conexión avisando a la otra parte con 30 días de antelación de su intención de hacerlo. Ninguna disposición del Acuerdo de Conexión altera los poderes y responsabilidades legales del NWS o del Usuario. Este Acuerdo está pensado para facilitar dichos poderes a través de acción cooperativa. En caso de un incidente de seguridad, el NWS podrá terminar este Acuerdo de Conexión sin brindar aviso razonable al Usuario.

SECCIÓN 13 - TÉRMINOS DEL ACUERDO

Este Acuerdo de Conexión permanecerá en efecto por un período de cinco (5) años después de la última fecha indicada en la sección de firmas que aparece a continuación. Después de cinco (5) años, este acuerdo se vencerá sin ninguna acción adicional. Si el NWS y el Usuario desean renovar este Acuerdo de Conexión, podrán hacerlo examinando el documento, actualizándolo si fuera necesario y volviendo a autorizarlo. El nuevo acuerdo firmado debe reemplazar explícitamente el presente Acuerdo de Conexión, al cual se deberá hacer referencia por título y fecha.

SECCIÓN 14 – AUTORIDAD FIRMANTE

Acepto los términos de este Acuerdo de Conexión del Usuario.

NOAA/NWS	Cliente de datos NOAAnet
Nombre: Craig Hegemann	Nombre:
Título: Propietario del sistema NOAAnet	Título:
Firma:	Firma:
Fecha:	Fecha:

APÉNDICE A: Lista de contactos para conexión de Usuario a NOAAnet del NWS

Contactos principales

OFICINA	ROL	NOMBRE	EMAIL	TELÉFONO	OTRA INFORMACIÓN
Programa NOAAnet del National Weather Service	Gerente del programa	Tom Sandman	Thomas.sandman@noaa.gov	(301) 713-0996 ext.221	
	Líder técnico	Phil Cragg	Phil.cragg@noaa.gov	(301) 713-0984 ext.216	
	Líder de ingeniería	Keith Myers	keith.myers@noaa.gov	(301) 713-1113 ext.195	
	Gerente de operaciones	Sue Murphy	Susan.murphy@noaa.gov	(301) 713-0864 ext.174	
Oficina del programa ISCS	Gerente del programa	Robert (Bob) Gillespie	robert.gillespie@noaa.gov	(301) 713-9478 ext.140 (240) 338-1203	
	Líder del programa	Patrick (Pat) Gillis	patrick.gillis@noaa.gov	(301) 713-1743 ext.104 (443) 421-0363	

Comunidad de usuarios del ISCS

ROL	NOMBRE	EMAIL	TELÉFONO	OTRA INFORMACIÓN
Gerente				
Personal técnico				
Persona que recibió el equipo				

APÉNDICE B: Controles físicos y ambientales (recomendaciones)

CONTROL DEL ACCESO FÍSICO

El Usuario debe establecer controles en todos los puntos de acceso físico (incluidos los puntos designados de entrada y salida) a las instalaciones que contienen los sistemas de información (a excepción de aquellas áreas de las instalaciones designadas oficialmente para acceso público) y verificar la autorización de acceso a nivel individual antes de permitir el acceso a las instalaciones. La organización controla el acceso a las áreas designadas oficialmente para acceso público, según sea apropiado, de acuerdo con la evaluación de riesgos de la organización. El Usuario debe controlar el acceso físico al equipo NOAAnet independientemente de los controles sobre el acceso físico a las instalaciones.

CONTROL DEL ACCESO AL MEDIO DE TRANSMISIÓN

Las protecciones físicas aplicadas a las líneas de distribución y transmisión de NOAAnet ayudan a impedir los daños accidentales, las interrupciones del servicio y cualquier manipulación o alteración física. Además, las protecciones físicas son necesarias para ayudar a impedir la interceptación furtiva o la modificación de las transmisiones no encriptadas en tránsito. Las posibles medidas de protección para controlar el acceso físico a las líneas de distribución y transmisión del sistema de información incluyen (i) cerrar los armarios de conexiones con llave; (ii) desconectar o trabar los enchufes auxiliares; y/o (iii) proteger los cables instalándolos en conductos o bandejas.

SUPERVISIÓN DEL ACCESO FÍSICO

El Usuario debe supervisar el acceso físico a los sistemas de información para detectar y responder ante cualquier incidente de seguridad. El Usuario debe supervisar las alarmas de intrusión y el equipo de vigilancia en tiempo real.

CONTROL DE VISITANTES

El Usuario debe controlar el acceso físico a los sistemas de información autenticando los visitantes antes de autorizar su acceso a las instalaciones o a cualquier área que no esté designada para acceso público. El Usuario debe escoltar a los visitantes y supervisar su actividad, cuando sea necesario.

REGISTROS DE ACCESO

El Usuario debe mantener constancia del acceso de los visitantes a la instalación donde reside el equipo de NOAAnet (a excepción de las áreas de las instalaciones designadas oficialmente para acceso público), que debe incluir: (i) nombre y organización del visitante; (ii) firma del visitante; (iii) documento de identificación presentado; (iv) fecha de acceso; (v) hora de entrada y salida; (vi) propósito de la visita; y (vii) nombre y organización de persona que recibió la visita. Los funcionarios designados dentro de la organización revisarán el registro de visitantes.

El Usuario debe emplear mecanismos automatizados para facilitar el mantenimiento y la revisión de los registros de acceso. El Usuario debe mantener un expediente de todo acceso físico, tanto para los visitantes como para el personal autorizado.

EQUIPO DE CORRIENTE Y CABLES DE ENERGÍA ELÉCTRICA

El Usuario debe proteger el equipo de corriente y los cables de energía eléctrica del equipo de NOAAnet para evitar su daño y destrucción. El Usuario debe emplear sistemas de cables de energía eléctrica redundantes y paralelos.

APAGADO DE EMERGENCIA

El Usuario debe instalar en lugares específicos dentro las instalaciones en las cuales se encuentren concentrados los recursos de sistema de información la capacidad de apagar la corriente de cualquier componente del sistema de información que pueda estar averiado o que pueda fallar sin necesidad de que el personal se le acerque, lo cual podría ser peligroso. El Usuario debe proteger la capacidad de apagar la corriente en casos de emergencias de la posibilidad de activación accidental o no autorizada.

ALIMENTACIÓN ELÉCTRICA DE EMERGENCIA

A corto plazo, el Usuario debe proporcionar una fuente de alimentación ininterrumpida para facilitar el cierre ordenado del sistema de información en caso de una pérdida del suministro de energía primario. A largo plazo, el Usuario debe instalar una fuente alternativa de alimentación autónoma para el sistema de información que sea capaz de mantener la capacidad operacional mínima necesaria en caso de la pérdida prolongada del suministro de energía primario.

PROTECCIÓN CONTRA INCENDIOS

El Usuario debe emplear y mantener dispositivos y sistemas de detección y supresión de fuego que se puedan activar en caso de incendio. El Usuario debe emplear dispositivos o sistemas de supresión de fuego que notifiquen automáticamente de su activación a la organización y al personal de emergencia.

CONTROL DE TEMPERATURA Y HUMEDAD

El Usuario debe mantener dentro de niveles aceptables y controlar a intervalos regulares la temperatura y la humedad en las instalaciones que contienen el equipo de NOAAnet.

PROTECCIÓN CONTRA DAÑOS CAUSADOS POR AGUA

El Usuario debe proteger el sistema de información contra los daños provocados por agua que puedan resultar de caños rotos u otras fuentes de derrame de agua asegurando que las llaves de paso principales sean accesibles y funcionen correctamente, y que el personal clave esté al tanto de ellas. El Usuario debe emplear mecanismos que protejan el equipo de NOAAnet contra daños provocados por el agua en caso de una fuga importante, sin necesidad de intervención humana.

ENTREGA Y RETIRO

El Usuario debe controlar los elementos relacionados con el sistema de información que entran y salen de las instalaciones y mantener constancia adecuada de dichos elementos.

UBICACIÓN DE LOS COMPONENTES DEL SISTEMA DE INFORMACIÓN

El Usuario debe colocar los componentes de NOAAnet dentro de la instalación de modo tal de reducir al mínimo el potencial de daño que puedan sufrir por peligros físicos o ambientales y reducir al mínimo la oportunidad de acceso no autorizado. Los peligros físicos y ambientales incluyen, entre otros, inundaciones, incendios, tornados, terremotos, huracanes, actos de terrorismo, vandalismo, interferencias eléctricas y la radiación electromagnética. Siempre que sea posible, la organización también debe considerar la ubicación o situación de las instalaciones con respecto a peligros físicos y ambientales.