## NIST SP 800-30 Rev. 1

## 

### **Guía para evaluar el riesgo**

NIST SP 800-30 es una publicación que proporciona orientación sobre la realización de evaluaciones de riesgos. Describe estrategias para identificar, analizar y remediar los riesgos. Las organizaciones utilizan NIST SP 800-30 para obtener información sobre la probabilidad y la gravedad potenciales de los riesgos, lo que les ayuda a tomar decisiones informadas sobre la asignación de recursos, la implementación de controles y la priorización de los esfuerzos de corrección.

Este documento de cuatro páginas es una adaptación de NIST SP 800-30 Rev. 1. El término "Rev. 1" significa que es la primera versión actualizada de esta publicación. De vez en cuando, el NIST revisa sus documentos para incorporar nueva información, reflejar los cambios en la tecnología y los requisitos normativos, o abordar los comentarios.

**Nota: El** Centro de Recursos de Seguridad Informática [del NIST](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)  contiene más información sobre SP 800-30 Rev. 1.

### **Fuentes de amenazas**

NIST SP 800-30 define y categoriza las fuentes de amenazas como entidades o circunstancias que pueden afectar negativamente a los sistemas de información de una organización. Esta información es útil para identificar y evaluar los riesgos potenciales. Al hacer referencia a él, tenga en cuenta la intención o las capacidades de las fuentes de amenazas internas y externas.

**Nota:** En la siguiente tabla se enumeran algunas posibles *fuentes de amenazas* que podrían poner en peligro un servidor de bases de datos de acceso público.

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Ejemplos** | **Descripción** |
|  | *Usuario estándar*   * Empleado * Cliente   *Usuario privilegiado*   * Administrador de sistemas   *Grupo*   * *Competidor* * Proveedor * Socio comercial * Estado nación   *Forastero*   * Hacker * Hacktivista * Amenaza persistente avanzada (APT) | Amenazas que surgen de individuos o grupos que podrían explotar los recursos cibernéticos de manera intencional o accidental. Por ejemplo, pueden alterar los datos de una manera que afecte negativamente a la empresa. Alternativamente, podrían robar datos intencionalmente y dañar el equipo comercial. |
|  | *Hardware*   * Almacenamiento * Tratamiento * Comunicaciones   *Software*   * *Sistema(s) operativo(s)* * Gestión de redes * Software malintencionado | Amenazas que se originan en factores no humanos. Por ejemplo, fallos de los equipos debido a la antigüedad, el agotamiento de los recursos u otras circunstancias. |
|  | *Entorno operativo*   * Controles de temperatura * Controles de humedad * Fuentes de alimentación defectuosas   *Peligros naturales*   * Cortes de energía * Fenómenos meteorológicos extremos | Amenazas que surgen de factores accidentales no humanos. Por ejemplo, fallos de equipos causados por el entorno operativo. |

### **Eventos de amenaza**

NIST SP 800-30 define y categoriza los eventos de amenaza como instancias reales en las que una fuente de amenaza explota una vulnerabilidad y causa daños o perjuicios a los sistemas de información de una organización. Esta información es útil para obtener información sobre los tipos de riesgos a los que se enfrentan los activos. Se pueden identificar controles y contramedidas más efectivos mediante la comprensión de posibles eventos de amenazas,

**Nota:** En la siguiente tabla se enumeran solo algunos posibles *eventos de amenaza* que podrían poner en peligro un servidor de base de datos de acceso público.

|  |  |
| --- | --- |
| **Ejemplos** | **Descripción** |
| Realizar el reconocimiento y la vigilancia de la organización | La fuente de amenazas examina y evalúa las vulnerabilidades de la empresa a lo largo del tiempo utilizando varias herramientas (por ejemplo, escaneo, observación física). |
| Obtener información confidencial a través de la exfiltración | La fuente de amenazas instala software malintencionado en los sistemas de la organización para localizar y adquirir información confidencial. |
| Modificar/Eliminar información crítica | El origen de la amenaza altera o elimina datos que son críticos para las operaciones comerciales diarias. |
| Elabora certificados falsos. | El origen de la amenaza compromete una autoridad de certificación para que sus conexiones parezcan legítimas. |
| Instale rastreadores de red persistentes y dirigidos en los sistemas de información de la organización. | La fuente de amenazas instala software diseñado para recopilar (rastrear) el tráfico de red durante un período de tiempo continuo. |
| Llevar a cabo ataques de denegación de servicio (DoS). | La fuente de amenazas envía solicitudes automatizadas y excesivas para abrumar las capacidades operativas del sistema. |
| Interrumpa las operaciones de misión crítica. | El origen de la amenaza compromete la integridad de la información de tal manera que impide que la empresa lleve a cabo operaciones críticas. |
| Ofusca futuros ataques. | La fuente de amenazas toma medidas para inhibir la efectividad de los sistemas de detección de intrusiones o las capacidades de auditoría en la empresa. |
| Llevar a cabo ataques de "intermediario". | El origen de amenazas escucha las sesiones entre sistemas internos y externos. Más tarde, transmiten mensajes entre la organización y los sistemas externos que les hacen creer que están hablando directamente entre sí a través de una conexión privada. |

## Probabilidad de un evento de amenaza

En general, la *probabilidad* de un evento de amenaza debe ser una puntuación basada en una combinación de factores. Por ejemplo, cualquier evidencia disponible que tenga, experiencia previa y su juicio experto.

Tenga en cuenta la intención o las capacidades de un origen de amenaza y los posibles eventos de amenaza al producir una puntuación de probabilidad.

|  |  |  |
| --- | --- | --- |
| **Valores cualitativos** | **Valores cuantitativos** | **Descripción** |
| Alto | 3 | Es casi seguro que el origen de la amenaza iniciará un evento de seguridad. Un evento puede tener efectos múltiples, graves o catastróficos en las operaciones y los activos comerciales. |
| Moderado | 2 | Es probable que el origen de la amenaza inicie un evento de seguridad. Un evento podría reducir significativamente la funcionalidad de las operaciones y los activos de la organización. |
| Bajo | 1 | Es muy poco probable que el origen de la amenaza inicie un evento de seguridad. Un evento podría tener efectos menores e insignificantes en las operaciones comerciales y los activos. |

## Gravedad de un evento de amenaza

En general, la *gravedad* de un evento de amenaza es una medida de su impacto potencial en las operaciones empresariales. Por ejemplo, ¿el evento haría que una función de negocio se detuviera por completo? ¿Podría interrumpir temporalmente un proceso de negocio y pasar desapercibido?

Tenga en cuenta el impacto empresarial de los eventos de *amenazas* al generar una puntuación de gravedad.

|  |  |  |
| --- | --- | --- |
| **Valores cualitativos** | **Valores cuantitativos** | **Descripción** |
| Alto | 3 | Es casi seguro que el origen de la amenaza iniciará un evento de seguridad. Un evento puede tener efectos múltiples, graves o catastróficos en las operaciones y los activos comerciales. |
| Moderado | 2 | Es probable que el origen de la amenaza inicie un evento de seguridad. Un evento podría reducir significativamente la funcionalidad de las operaciones y los activos de la organización. |
| Bajo | 1 | Es muy poco probable que el origen de la amenaza inicie un evento de seguridad. Un evento podría tener efectos menores e insignificantes en las operaciones comerciales y los activos. |